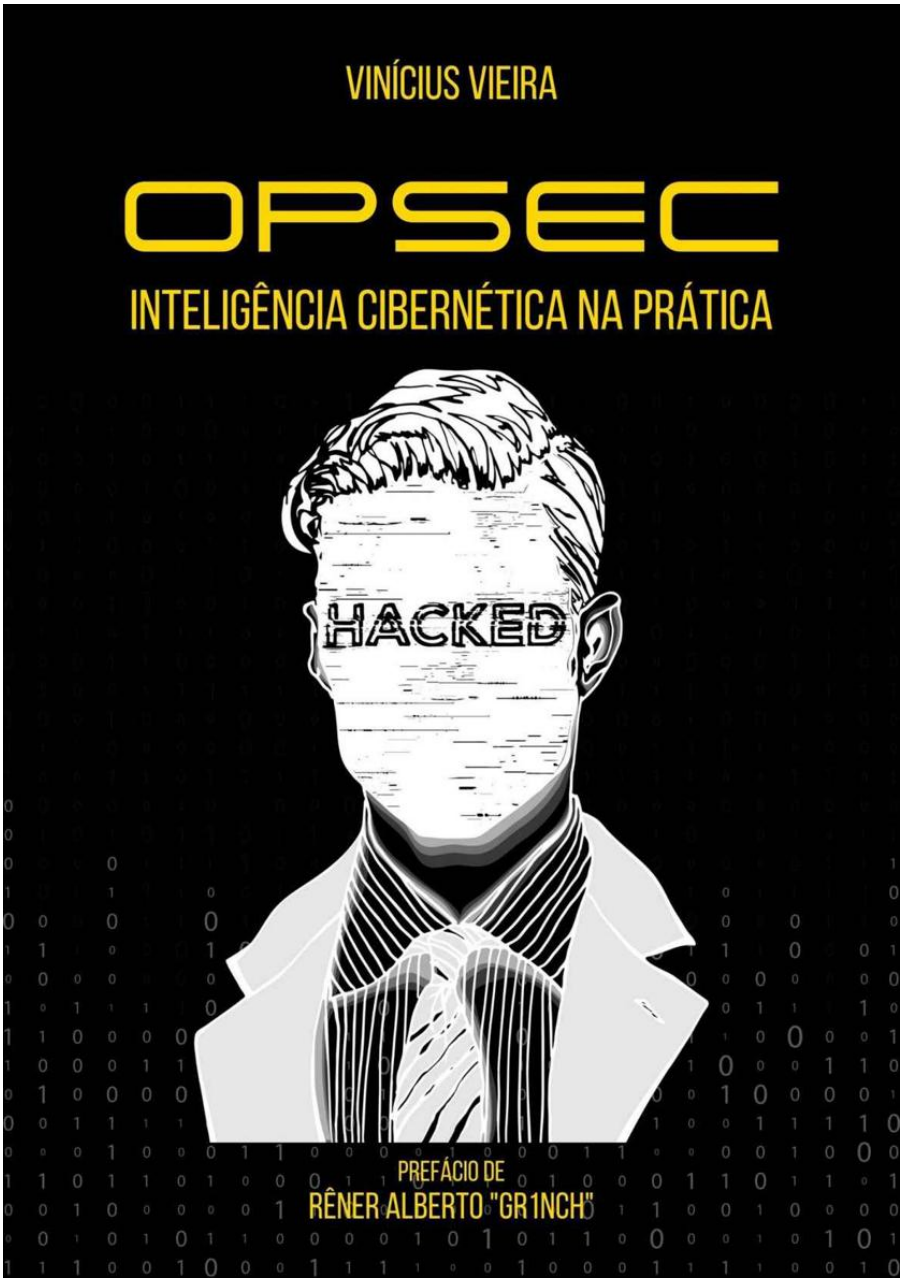
OPSEC, Inteligência Cibernética na Prática

Vinícius Vieira



OPSEC

Inteligência Cibernética na Prática

Vinícius Vieira

2022

Sobre o Autor

Vinícius Vieira é pesquisador de cyber security e professor. É

coordenador acadêmico nos cursos de Graduação Tecnológica em Defesa Cibernética e no MBA em Cyber Security no Centro Universitário FIAP, em São Paulo. Autou por mais de 18 anos na área de segurança cibernética das Forças Armadas, tendo se especializado em Guerra Cibernética e Cyber Intel. É mestre em Tecnologias Emergentes, especialista em Ethical Hacking, possui algumas certificações em Linux, Incident Handler e Segurança Ofensiva, bem como algumas CVE e exploits publicados.

Contents

OPSEC

Sobre o Autor

Prefácio

Introdução

Princípios da Inteligência

A Produção do Conhecimento

Low Profile as a Lyfestyle

Segurança como Valor Estratégico

Engenharia Social

Programação Neurolinguística

Praticando o PNL: Rapport e Âncora

Técnicas de Argumentação e Convencimento

Fundamentos da Anonimização

Fingerprint

Conhecendo as camadas da Internet

Rede Tor

Rede Privada Virtual (VPN)

Freenet

Invisible Internet Project (I2P)

Acessando a Dark Net através do Tor Browser

Acessando a Dark Net através da I2P

Acessando a Dark Net através da Freenet

Anonimização com SPLITTER

Open Source Intelligence (OSINT)

Técnicas de Busca de Dados Negados

Conclusão

Referências

Prefácio

Olá!

Minha missão aqui é tentar explicar a importância desse livro para você. O autor dessa obra possui um público muito grande de pessoas que são iniciantes no universo da segurança da informação, e quando ele me deu a missão de escrever esse prefácio eu me lembrei de todas as conversas que tivemos sobre a importância de construirmos uma base sólida de conhecimento. Então vamos começar com o cenário

atual em que vivemos e porque a segurança da informação e a privacidade se tornaram um estilo de vida. Sim! Segurança da informação e privacidade é muito mais do que um assunto de nerds. É

um estilo de vida.

Vivemos em um mundo conectado e não conseguimos imaginar nossas vidas sem os sistemas informatizados que hoje controlam o mundo que conhecemos. Adotamos um estilo de vida digital e cada vez mais o mundo real e o virtual passam a ser tão dependentes que as vezes é possível confundir e termos dificuldades para distinguir o real e o virtual. Um exemplo disso são os avanços da computação gráfica e da realidade virtual.

A raça humana é famosa por se adaptar as condições mais adversas e distintas. A vida humana se desenvolve, adapta e se fortifica perante os desafios aos quais lhe é imposta. Seria esse o segredo do sucesso da nossa espécie? Seria a nossa capacidade de adaptação aos novos ambientes o motivo pelo qual nossa evolução e adaptação foi tão bem-sucedida aos longos dos milhares de anos?

Nossa raça está se adaptando ao mundo no qual as máquinas e os sistemas informatizados desenvolvidos pela raça humana nos levaram a um ponto sem volta. Não é mais possível termos a mesma qualidade de vida sem depender das máquinas e das tecnologias que

criamos. Não é mais possível parar o desenvolvimento tecnológico.

Atingimos um ponto sombrio da história da nossa espécie onde VIDAS HUMANAS, assim como nossa segurança e integridade física, passaram a ser dependentes de sistemas informatizados em um mundo cada vez mais conectado. Pare um pouco para pensar nas consequências de “um ataque hacker”.

No sistema computadorizado que controla o tráfego aéreo dos aeroportos. Imagine o que acontece se esse tipo de sistema fosse simultaneamente comprometido em diferentes aeroportos por algum grupo terrorista com intenções claras de causar mortes. Esse tipo de ataque pode fazer com que os pilotos recebam informações erradas sobre as condições de pouso e decolagem, ou até mesmo o posicionamento real das demais aeronaves sobrevoando um mesmo espaço aéreo. Claramente um cenário de possíveis colisões de aeronaves em solo ou em voo pode se concretizar.

Imagine um ataque contra o sistema que controla o sincronismo dos semáforos de uma grande cidade. Quantas vítimas fatais em acidentes

de trânsito teríamos se esse sistema e suas integrações fossem comprometidos? Imagine todos os cruzamentos com apenas o sinal verde habitado ao mesmo tempo para todos os motoristas nos cruzamentos de vias de trânsito rápido. Seria possível evitar as colisões fatais?

E se o ataque fosse no sistema que controla a abertura e o fechamento das comportas de grandes represas próximas a grandes centros urbanos? Se sistemas assim fossem comprometidos dando vazão a um volume muito grande de água em curto espaço de tempo, o volume excessivo e inesperado de água poderia destruir cidades. As consequências podem ser semelhantes aos incidentes ocorridos em Minas Gerais no rompimento das barragens de Mariana no dia 05 de novembro de 2015 e de Brumadinho em 25 de janeiro de 2019.

Por fim imagine um “ataque hacker” no sistema que controla o

status de monitoramento dos reatores de uma usina nuclear. Se esses sistemas fossem adulterados para exibir informações imprecisas podendo gerar situações de instabilidade no núcleo dos reatores.

Poderíamos ter acidentes fatais semelhantes ao acidente de Chernobyl em 26 de Abril de 1986. Ataques assim entraram para a história como foi o caso do malware Stuxnet em 2010.

O mundo digital que a raça humana criou, passou a controlar o nosso mundo real. O problema é que as guerras do mundo digital não respeitam as fronteiras físicas do mundo real e vidas humanas podem ser perdidas em consequências que vão além desse estranho limite que existe entre o digital e o real.

O mercado de trabalho está cada vez mais aquecido em uma busca desesperada por profissionais com capacidade para proteger as fronteiras que se formaram no mundo digital. Os jornais e meios de comunicação falam com frequência sobre as consequências no mundo real dos ataques que aconteceram no mundo virtual.

Profissionais de áreas relacionadas a segurança da informação e privacidade são o objeto de disputa e desejo das empresas. Os prejuízos e as consequências que um ataque cibernético pode ter contra as empresas, ensinaram a elas que vale a pena investir em profissionais qualificados nessas áreas.

O problema é que o mercado de trabalho está ficando saturado de falsos especialistas em segurança da informação e privacidade.

Pessoas que não possuem uma base técnica sólida, mas dizem dominar as técnicas de invasão e defesa.

Temos que desenvolver novos hábitos para consolidar boas práticas no nosso estilo de vida em segurança cibernética e privacidade. Precisamos tomar o cuidado para não sermos comparados ou confundidos com os falsos profissionais que infestaram as redes sociais.

Seja bem-vindo a essa jornada de conhecimento, não tenho

dúvidas de que essa obra literária vai agregar muito e te ajudar a entender melhor muitos dos conceitos que são predominantes no universo da segurança da informação e da privacidade.

Rêner Alberto (aka Gr1nch)

Vieira, Vinícius
OPSEC : inteligência cibernética na prática /
Vinícius Vieira. -- São Paulo : Ed. do Autor, 2022.

Bibliografia.
ISBN 978-65-00-38498-7

1. Cibernética 2. Cibernética - Medidas de segurança 3. Gestão do conhecimento 4. Inovação tecnológica 5. Programação neurolinguística 6. Tecnologia I. Título.

22-99348 CDD-005.8

**Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)**

Índices para catálogo sistemático:

1. Internet : Segurança cibernética : Processamento de dados 005.8

Aline Graziele Benitez - Bibliotecária - CRB-1/3129

Agradeço ao meu Deus por ter chegado até aqui, sem Ele nada do que vivi seria possível!

Eu dedico esta obra a minha maravilhosa esposa e meus incríveis filhos, que sempre me incentivaram e estiveram ao meu lado em todos os momentos.

Introdução

A indefinição de ameaças, bem como o ressurgimento de fenômenos de grande repercussão nacional e internacional, como por exemplo o terrorismo e o crime organizado, a proliferação de ameaças no campo cibernético; tais como ataques, vazamento de dados e insiders, demandam respostas imediatas e pontuais com o mínimo de efeitos colaterais.

Para que uma empresa ou instituição possa atuar nesse ambiente difuso, é preciso compreender, o mais cedo possível, que a Segurança da Informação não é apenas um problema de TI. A cultura organizacional das corporações tende a deixar de lado os investimentos em Segurança da Informação, ação esta que tem levado importantes empresas a colherem péssimos frutos.

A existência de normas e procedimentos claros de segurança da informação, que deverão ser seguidos por todos os usuários da empresa, devem ser uma realidade coordenada a nível de direção e não somente como carácter informativo; haja vista que a maior dificuldade das grandes organizações é assegurar que todos os seus colaboradores conheçam e sigam corretamente as normas e políticas de segurança, entendendo a sua importância e colocando-as em prática.

O entendimento e a aplicação dos conhecimentos em Inteligência e Contrainteligência são vitais para o modelo de negócios de qualquer empresa, principalmente na sua vertente preditiva, permitindo que a direção possa ter um constante entendimento situacional, tanto das ameaças iminentes quanto das oportunidades de obtenção de vantagens comerciais.

Mas o que seria OPSEC, então?

OPSEC é um acrônimo para Operation Security (Operações de Segurança, em tradução literal), termo criado pelo Exército dos EUA e que surgiu durante a Guerra do Vietnã.

As ações de OPSEC foram criadas como um processo de identificação de informações para determinar se a inteligência adversária poderia observar ações amistosas e determinar se as informações obtidas pelo

adversário podem ser interpretadas como úteis para o inimigo ou não, e então tomar ações selecionadas para eliminar ou reduzir a exploração de informações adversas.

Há quem diga que a OPSEC se debruça somente sobre o campo da Contrainteligência, porém ao examinarmos minuciosamente o documento da NSA que introduz o tema – Purple Dragon: The Origin and Development of the United States OPSEC Program, temos a clareza de que as ações de OPSEC foram cruciais no processo de produção de conhecimento, não só sobre o adversário, mas principalmente no levantamento dos pontos de vulnerabilidade do Exército dos EUA durante a Guerra do Vietnã, tendo sido um artefato extremamente útil tanto para produção de conhecimento quanto para proteção de informações. Logo, poderíamos afirmar que a OPSEC é nada mais que a materialização das táticas de Inteligência e Contrainteligência através de técnicas e processos práticos.

Durante a leitura deste livro você irá reparar que muito dos termos e conceitos aqui apresentados possuem uma influência militar muito grande. E não era pra menos, haja vista que este tema surgiu muito antes de falarmos de Cyber Security, por exemplo. Desde as primeiras guerras da humanidade (incluindo as epopéias bíblicas, como é o caso dos espias que Moisés enviou à Canaã) a área de inteligência vem sendo forjada e amadurecida nos quartéis, até o ponto onde entendeu-se que estes conhecimentos seriam úteis para o campo cibernético.

Independente do seu posicionamento político quanto as guerras, existe um fato inegável: a indústria bélica é pioneira em avanços tecnológicos e científicos. Poderíamos tomar aqui diversos exemplos

para esta afirmação, mas se atendo ao campo da tecnologia podemos citar Allan Turing – conhecido como o pai da computação, que através de uma guerra (mais especificamente a II Guerra Mundial) pode colocar em prática o seu paper, materializando o modelo abstrato que era a Máquina de Turing na máquina eletromecânica Enigma, que foi responsável por decifrar códigos encriptados. E não só ele, mas a própria Rede Mundial de Computadores, que só foi possível através do projeto DARPANet desenvolvido pela Defense Advanced Research Projects Agency (DARPA) – uma agência de pesquisas especiais ligada ao Departamento de Defesa dos EUA.

Ou seja, boa parte do que temos hoje no que diz respeito a Tecnologia da Informação, e podemos até dizer no campo da Segurança da Informação, foi criado (ou minimamente sofreu influência) dos meios militares.

É fato que, por motivos óbvios, as técnicas e táticas militares de inteligência não ganharam capilaridade nos meios civis. Porém note que existe uma diferença entre “ganhar capilaridade” e “estar guardada em segredo”. E o nosso intuito neste livro é correlacionar conceitos, técnicas e táticas utilizadas em ações OPSEC para que você possa usufruir destes ensinamentos em seu dia-a-dia.

Neste livro discorreremos sobre os campos da Inteligência e Contrainteligência no que tangem ao ciberespaço, e principalmente, aprenderemos a utilizar estes conhecimentos para protegermos ou obtermos informações sensíveis às nossas organizações, sejam através de meios tecnológicos ou explorando vulnerabilidades humanas.

Princípios da Inteligência

Por mais que ao primeiro momento os termos sejam facilmente associados aos filmes de espionagem e conspirações, a atividade de inteligência nada mais é que a produção (Inteligência) e proteção (Contrainteligência) de conhecimentos e dados em que uma corporação tem interesse em obter ou preservar, respectivamente.

Logo, obter informações que possam dar vantagem política, estratégica ou comercial frente a concorrência, ou contribuir para uma maior segurança aos seus dados de valor é o foco principal.

Se fizermos uma análise superficial do tema “inteligência” e seus impactos no campo cibernético podemos concluir que o mundo vem convivendo com uma uma ampla gama de ameaças que vão desde o simples prazer de contornar barreiras de sistemas (sem más intenções aparentes) até crimes com propósito claros de danificar e expor países e organizações.

Sob este aspecto, identificar a origem desses atos, em face da capilaridade da rede mundial de computadores (além de outros aspectos técnicos, os quais iremos abordar mais pra frente) é uma tarefa árdua, principalmente por ser um campo onde não se tem definido claramente o conceito de “fronteira”.

Em outras palavras, não basta para uma organização possuir um time de defesa cibernética que domine os aspectos técnicos. Se esta não possuir a cultura de inteligência e contrainteligência atreladas ao seus processos de Segurança da Informação (ações de OPSEC), seus dados de valor não estariam somente vulneráveis mas também suas oportunidades de obtenção de vantagens frente a concorrência seriam escassas ou nulas, uma vez que os dados de diversas organizações

estão disponíveis de forma insegura na internet e/ou as barreiras de proteção destes dados são efêmeras.

A Produção do Conhecimento

Segundo Setzer(1999), podemos definir dado como uma sequência de símbolos quantificados ou quantificáveis, tais como letras, imagens, sons e etc, pois todos podem ser quantificados a ponto de alguém que entra em contato com eles ter eventualmente dificuldade de distinguir a sua reprodução, a partir da representação quantificada, com o original. É muito importante notar-se que qualquer texto constitui um dado ou uma sequência de dados, mesmo que ele seja ininteligível para o leitor.

Por sua vez a informação é uma abstração informal que representa algo significativo para alguém através dos dados (textos, imagens, sons e etc). Por exemplo, a frase "Paris é uma cidade fascinante" é um exemplo de informação - desde que seja lida ou ouvida por alguém, desde que "Paris" signifique a capital da França e "fascinante"

tenha a qualidade usual e intuitiva associada com aquela palavra.

O correto entendimento do dado processado é essencial para o planejamento e execução das tomadas de ação em uma organização, desde o nível operacional até o nível de direção. As informações são o resultado do processamento, manipulação e organização de dados.

Essas informações, se consideradas relevantes, são analisadas e transformadas em conhecimento. Esse conhecimento é fundamental para que os decisores possam ter um melhor entendimento da situação, contribuindo para o entendimento amplo dos cenários apresentados.

Outro fator importante sobre a inteligência, ou seja, sobre a produção de conhecimento, é a forma como o dado ou a informação é obtida. E apesar das divergências conceituais entre as linhas militares que se deseje seguir, existem basicamente dois tipos de formas de obtenção de informação: a coleta e a busca.

Quando falamos em coleta estamos nos referindo ao acesso ou a obtenção de dados disponíveis publicamente, mesmo que somente acessíveis através de técnicas de buscas avançadas.

Um exemplo claro da coleta é a obtenção de dados através de buscas

na

internet,

informações

em

redes

sociais

e

o

correlacionamento destes para produzir uma informação.

Digamos que o usuário X tem seu CPF disponível numa publicação de um Diário Oficial, publicado na internet. E, através de uma busca em redes sociais, é possível chegar no nome completo da sua mãe e sua data de nascimento. Com o correlacionamento destas informações seria possível, por exemplo, consultar o status do CPF na Receita Federal ou ainda sua situação eleitoral. Tudo isso através de dados coletados em fontes públicas.

No entanto, quando falamos da busca, estamos nos referindo a obtenção de dados e informações que não estejam disponíveis publicamente. Um exemplo claro é quando, através de uma ação de Engenharia Social, ou através da exploração de uma vulnerabilidade em um sistema, se tem acesso aos dados bancários de um indivíduo.

Esta diferenciação é importantíssima, pois ela será a linha tênue entre realizar uma ação criminosa ou não. É amplamente possível um civil realizar ações de busca de informações, como por exemplo dentro de Pentests ou atividades de Red Team, os quais estão amparados em um contrato com a permissão explícita para a execução deste tipo de atividade. Inclusive este mindset ofensivo é fundamental para os profissionais destas áreas.

E como diria o Tio Ben: “Com grandes poderes vem grandes responsabilidade”. Pense nisso!

Outro fator importante, além da forma como o dado é obtido, são as fontes de Inteligência, as quais são classificadas de acordo com a natureza e a proveniência dos dados que elas fornecem.

Alguns acrônimos são usados para definir esses tipos de inteligência

com base na sua procedência. Os tópicos que seguem trazem uma breve descrição dos principais tipos de fontes de inteligência.

a) **Human Intelligence** - Inteligência Humana - descreve um tipo de inteligência derivada a partir de informações coletadas e fornecidos por fontes humanas. Obtido por meio de interrogatórios, depoimentos e entrevistas. É o tipo mais básico de inteligência, pois requer apenas capital humano especializado para a sua coleta e dispensa o alto custo de uma operação de campo.

b) **Signals Intelligence Measurement and Signatures Intelligence** – inteligência de medição e assinaturas – é o termo que define a inteligência obtida de medidas e assinaturas de eventos químicos ou físicos, como por exemplo de um incêndio.

c) **Cyber Intelligence/Digital Network Intelligence** –

Inteligência Cibernética/Inteligência de Redes Digitais – refere-se a inteligência obtida do ciberespaço. Bastante difundida atualmente e dentro dela insere-se outros tipos de inteligências, tais como a OSINT, HUMINT e Threat Intel, por exemplo.

d) **Open Source Intelligence** - ou inteligência de fontes abertas (OSINT) é definido como inteligência derivada de informações publicamente disponíveis, bem como outras informações não classificadas, isto é, cujo conteúdo não possui caráter sigiloso e pode ser conhecido por qualquer pessoa.

Entendido as diferenças entre as ações de OPSEC, bem como os seus objetivos e benefícios, precisamos conceituar os princípios que devem nortear a atividade de inteligência em uma organização:

- Segurança: Em todas as fases de sua produção, o conhecimento deve ser protegido de forma que o seu acesso seja limitado apenas às pessoas credenciadas;

- Objetividade: Para que seja útil, o conhecimento deve ter sua

produção orientada a objetivos claramente definidos;

- Clareza: Os conhecimentos produzidos devem ser expressos de forma a receberem imediata e completa compreensão por parte dos receptores;

- Imparcialidade: A produção de conhecimento deve se identificar com as ideias preconcebidas, subjetivismos e outras influências que possam

gerar distrações;

- Precisão: Deve-se procurar atingir o maior grau de exatidão da obtenção de dados e na produção de conhecimentos;

- Continuidade: A necessidade de conhecimento é permanente. As atividades de inteligência e contrainteligência são executadas constantemente e ininterruptamente; e

- Predição: A inteligência deve informar acerca do que as ameaças e oportunidades podem provocar, procurando antecipar-se sempre.

Low Profile as a Lyfestyle

Você já parou pra analisar o quanto da sua vida é exposta nas redes sociais? Ou melhor, quantos dos seus “amigos” virtuais são seus amigos de verdade, ou ao menos são pessoas que conhece pessoalmente, sabe onde moram e etc? Quando você recebe uma nova solicitação de amizade, quais critérios você utiliza pra decidir adicionar ou não?

Se após essa análise você começou a se preocupar com sua privacidade, realmente você precisa entender o conceito de Low Profile as a Lifestyle. E se por acaso você não tem rede social, ou sabe que, baseado nas respostas dos questionamentos acima a sua privacidade está “assegurada”, continue lendo pois você poderá enxergar que não está tão bem quanto acha que esteja.

Somos uma geração de indivíduos que sabe muito pouco sobre o significado de privacidade. E se sabemos de forma conceitual, na prática, inconscientemente não damos a mínima para a importância dela em nossas vidas - até pra nossa segurança pessoal. Não é novidade pra ninguém que os grandes players na Internet nos usam como massa de manobra diariamente e temos cada vez mais caminhado como gado para um fim extremamente perigoso, onde a única referência que teremos da privacidade será nos dicionários.

Diversos estudos científicos, pesquisas e até documentários –

como por exemplo “O Dilema das Redes”, que estreou no Netflix, vem nos alertando sobre os perigos das redes sociais. E aqui eu trago uma reflexão: será que o problema estaria somente em nossa vida online?

É fato que, como humanidade, estamos tendo cada vez mais vida social online do que presencialmente e a própria pandemia potencializou muito isso. Avançamos nesse sentido em dois anos o que

talvez levaríamos 10. Já estamos vivendo o início do Metaverso,

empresas comprando terrenos online, reuniões sendo feitas através de avatares e até eventos de entretenimento ocorrendo completamente nestes espaços virtuais.

Irei recolocar meu questionamento anterior de forma mais clara: será que o perigo reside somente na vida virtual ou ela é um reflexo do que somos em nossas interações pessoais?

Quando falamos de Low Profile estamos falando de indivíduos que entendem os benefícios (e a importância) de viver "fora dos holofotes", que entendem que sua privacidade é um dos seus maiores bens e primam por ela a todo custo, tomando sempre cuidado em não expor suas vidas pessoais.

Uma certa vez eu tive o seguinte diálogo com um amigo:

- "Vinícius, você já comeu ovo de pata?"

- … não, não que me lembre. Por que?

- "Você sabia que o ovo da pata é muito mais gostoso que o ovo da galinha?"

- Realmente não sabia…

- "E você sabe por que as pessoas consomem muito mais ovos de galinha do que de pata?"

- Sinceramente não sei… na verdade nunca parei pra pensar sobre.

- "Pois é… comemos mais ovos de galinha do que de pata, pois a galinha faz barulho quando coloca os seus ovos. Já a pata não… dai quando vamos ver, o ovo já virou um patinho"

Eu confesso que essa conversa marcou a minha vida. O que meu amigo quis me ensinar foi que, na vida, não podemos abrir nossos tesouros para os outros. Ninguém precisa saber o que você está fazendo, onde está jantando ou viajando, seus projetos e planos para o futuro e etc. Tudo isso são informações muito importantes pra nós e que precisam, a todo custo, estarem resguardadas pela nossa privacidade.

A Inteligência Militar prega que o "agente de Inteligência é o soldado do silêncio", justamente pois quanto mais ouvirmos (e falarmos

menos) mais teremos controle das informações que compartilhamos. Como operador de OPSEC é imprescindível que você internalize esse conceito, e mais: use isso como estilo de vida! Não adianta você usar esta técnica no seu dia-a-dia se a sua família, principalmente os mais próximos, como esposa e filhos, não o fazem.

Eu pessoalmente já atuei em casos em que coletamos muitas informações sensíveis de determinados alvos através das redes sociais de familiares.

Abaixo vou citar alguns princípios importantes sobre esse mindset:

- Pense sempre antes de falar. Não aja por impulso.

- Compartimente a informação. Você não precisa falar tudo, somente o necessário. Não entre em detalhes que não dizem respeito aos demais.

- Ninguém precisa saber sua rotina além das pessoas que moram com você.

- As paredes tem ouvidos. Assuntos que não dizem respeito aos outros não podem ser falados fora de casa. Não fale sobre onde vai ou o que vai fazer em um hall de apartamento ou no quintal da sua casa.

- Se quiser ter rede social, veja mais e poste menos.

- Separe suas redes sociais pessoais das profissionais. Seu LinkedIn não é seu Facebook!

- Ensine estes princípios para sua família. Ajude-os pois assim você está protegendo a sua segurança e a deles.

Nos próximos capítulos abordaremos alguns temas que lhe farão refletir sobre o Low Profile as a Lifestyle, pois você verá os perigos que nos rondam a todo momento na Internet (e como se proteger

contra eles), bem como a importância de termos cuidado com o que compartilhamos em nossas relações interpessoais.

Segurança como Valor Estratégico

Tal como acontece com todos os bens valiosos, a informação também precisa ser protegida. No entanto, toda salvaguarda tem um custo e portanto ao determinar quais salvaguardas proteger, deve-se levar em consideração a seguinte expressão:

Valor da Informação >= Custo da Proteção

Para satisfazer essa expressão é necessário conhecer tanto o valor da informação quanto o custo de protegê-la. O custo da proteção está atrelado aos recursos tangíveis utilizados tais como: tecnologia, material e pessoas. Portanto seu cálculo, embora não seja trivial, provavelmente será estabelecido. Por outro lado determinar o valor da informação é algo razoavelmente complicado pois se trata de atribuir valor a um ativo intangível. (CÔRTE, 2014)

Portanto quando a informação não é valorizada ou (é valorizada de forma inadequada) a proteção dessa informação pode se tornar inconsistente. Quando o valor de uma informação não é estimado corretamente sua proteção pode ser super dimensionada ou sub dimensionada. Portanto, definir o nível de proteção que se pretende dar à informação é muito mais assertivo quando ela passa por um processo de classificação.

Este processo inclui determinar o nível de proteção que cada dado deve receber. Por exemplo, (em tese) a folha de pagamentos de uma empresa devem ter um nível de proteção mais alto do que uma lista interna de números de telefone de um determinado setor. Note que ao frisar “em tese” estou deixando subentendido que cada caso é um caso, ou seja, se essa lista telefônica contém um determinado número onde somente certas pessoas dentro da organização tem acesso, ao cair em mãos erradas, poderia servir de asset para um ataque de Engenharia Social, por exemplo.

A ISO 27001 possui uma lista de práticas recomendadas para a classificação das informações. E sabendo que nosso objetivo aqui não é abordar o tema por este viés, gostaria de falar sobre uma outra forma de classificar informações.

Lembra que comentamos que a inteligência visa obter dados, enquanto a contrainteligência visa proteger dados? Pois bem, quando falamos das boas práticas de classificação de informação baseada na ISO 27001 estamos falando de proteger nossos dados e informações, ou seja, estamos atuando no campo da Contrainteligência. E se ao invés de nos preocuparmos em classificar os nossos dados, nós precisássemos classificar os dados que estamos obtendo?

Vamos visualizar o seguinte cenário para facilitar o entendimento: imagine que você atua numa área de Cyber Intel e, durante uma ação de coleta de dados, você teve acesso a um leak de usuários e senhas da sua empresa. Qual seria a veracidade destas informações? Estes usuários e senhas realmente são da sua empresa? Eles ainda funcionam?

Ao efetuar estes tipos de pergunta estamos avaliando a informação em si, ou seja, o quanto ela é fidedigna. E se as perguntas forem diferentes… digamos que a informação é sim verdadeira, são credenciais ainda ativas da sua empresa. Logo a fonte da qual você obteve esta informação foi confiável. Mas ela é uma fonte nova, ou seja, você ainda não havia conhecido esta fonte? E se esta fonte já é conhecida, porém nem sempre ela lhe traz informações verdadeiras?

Note que, ao fazer estas perguntas eu estou avaliando a fonte de onde eu obtive a informação, e não mais a informação em si.

Nos meios militares existem sistemas métricos para avaliar, tanto a fonte quanto a informação. Obviamente que não cabe aqui discorrer sobre estes sistemas, pois o nosso objetivo é entender que durante uma ação de inteligência (obtenção de informações) eu preciso classificar tanto a informação quanto a fonte em si, pois baseado nesta classificação, eu poderei gerar conhecimento ao meu tomador

de decisão para que o mesmo tenha a visão do risco e/ou ameaça ao meu negócio.

Engenharia Social

Viver em um mundo conectado onde todas as nossas atividades cotidianas são permeadas pela tecnologia, apesar de trazer incríveis benefícios, como automatizações de processos, facilidades em acesso à informação de forma ágil e continuada, possibilidade de comprar e efetuar pagamentos sem sair de casa ou ainda ter que andar com dinheiro, dentre outros, também nos expõe a riscos que muita das vezes não concebemos.

Ao ouvir sobre golpes na internet, fraudes eletrônicas, roubo e vazamento de dados, imaginamos que os alvos destes tipos de ataques são, em sua maioria, empresas e instituições de governos que possuem dados valiosos ou segredos comerciais, porém esquecemos que toda organização, e aqui entenda uma Pessoa Jurídica, é constituída por pessoas que, assim com nós, tem seus dados expostos de forma displicente na internet. Outro fator preponderante nesse cenário é que assim como pessoas precisam de outras pessoas para se relacionar e estabelecer relações dos mais diversos tipos, no mundo corporativo, empresas também dependem de outras empresas para sobreviver, sejam elas fornecedores, parceiros comerciais, revendedores e até concorrentes.

Mas o que tudo isso tem a ver com Engenharia Social? A engenharia

social é a atividade que visa obter acesso a informações importantes ou confidenciais em organizações ou sistemas, enganando ou tirando proveito da confiança das pessoas. Ela utiliza o conhecimento empírico e científico das relações humanas para manipular as vítimas para oter informações confidenciais e dados explicitamente negados (não disponíveis publicamente), bem como das organizações sociais e empresas nas quais a vítima está incluída.

Falando em números, a Verison, uma das grandes empresas no ramo de segurança digital, lançou em seu último relatório anual sobre

investigação de violação de dados (Data Breach Investigations Report 2021) dados interessantes: 93% dos dados vazados de empresas foram através de ataques de engenharia social; da lista dos 20 tipos de ataque mais utilizados no ano anterior, 3 se relacionavam com Engenharia Social; dentre as táticas mais utilizadas por atacantes para obter sucesso, 35% envolviam Engenharia Social; em relação as motivações dos atacantes, 59% foram para obter dados financeiros e em relação aos dados comprometidos, 47% eram dados pessoais.

Imaginemos uma empresa X que se preocupa com Segurança da Informação e investe pesado em ativos de segurança tais como Next Generation Firewalls, sistemas de autenticação centralizada, endpoint detection e response (EDR) e etc. Esta empresa ainda contrata rotineiramente times de análise de vulnerabilidades para testarem suas brechas com o intuito de uma melhoria contínua da segurança dos seus dados. Na sua concepção, esta empresa estaria segura contra ataques de Engenharia Social? Posso lhe afirmar seguramente que não! A Segurança da Informação sempre deverá tratar pessoas, processos e tecnologias. Se qualquer um destes pilares não for envolvido, inegavelmente não temos segurança.

Kevin Mitnik, preso em 1995 através de uma ação conjunta do FBI com a NSA e autor do Best Seller “A Arte de Enganar”, afirma em seu livro que “não existe tecnologia no mundo que evite o ataque de um Engenheiro Social”. Em sua obra ele afirma que o elo mais fraco em qualquer ecossistema de segurança somos nós: os seres humanos.

Seu livro está recheado de histórias que contam casos reais de hackers e Engenheiros Sociais (sim, nem todo Engenheiro Social é um hacker, pois em alguns cenários não é necessário conhecimento de tecnologia para se explorar vulnerabilidades em pessoas) que lograram êxito em ações contra grandes empresas por manipularem simples colaboradores. Nestes casos as pessoas exploradas não faziam ideia de que a informação que ela estava passando, para elas irrelevante

naquele momento, era mais uma peça de um grande quebra-cabeças que o Engenheiro Social estava montando com o intuito de realizar uma ação ainda maior.

O comportamento humano é o fator decisivo para um ataque da Engenharia Social pois é através dele que as vulnerabilidades de cada indivíduo são percebidas.

Segundo Coelho (2008) as pessoas possuem características psico comportamentais que as tornam vulneráveis a ataques de engenharia social que são:

- Vaidade pessoal e/ou profissional: o ser humano costuma ser mais receptivo a avaliação positiva e favorável aos seus objetivos, aceitando basicamente argumentos favoráveis a sua avaliação pessoal ou profissional ligada diretamente ao benefício próprio ou coletivo de forma demonstrativa.

- Autoconfiança: o ser humano busca transmitir em diálogos individuais ou coletivos o ato de fazer algo bem, coletivamente ou individualmente, buscando transmitir segurança, conhecimento, saber e eficiência, buscando criar uma estrutura base para o início de uma comunicação ou ação favorável a uma organização ou individuo.

- Formação profissional: o ser humano busca valorizar sua formação e suas habilidades adquiridas nesta faculdade, buscando o controle em uma comunicação, execução ou apresentação seja ela profissional ou pessoal buscando o reconhecimento pessoal inconscientemente em primeiro plano.

- Vontade de ser útil: o ser humano, comumente, procura agir com cortesia, bem como ajudar outros quando necessário.

- Busca por novas amizades: o ser humano costuma se agradar e sentir-se bem quando elogiado, ficando mais vulnerável e aberto a dar informações.

- Propagação de responsabilidade: trata-se da situação na qual o ser humano considera que ele não é o único responsável por um conjunto de atividades.

- Persuasão: compreende quase uma arte a capacidade de persuadir pessoas, onde se busca obter respostas específicas. Isto é

possível porque as pessoas possuem características comportamentais que as tornam vulneráveis a manipulação.

Ao explorar essas características os engenheiros sociais podem obter informações de interesse das organizações sem precisar comprometer os sistemas de segurança, roubar dados ou implantar malwares. Em outras palavras, um engenheiro social não precisa usar meios tecnológicos para perpetrar uma ação, embora o uso da tecnologia possa potencializar certos tipos de ataques.

Analisando uma ação de Engenharia Social do ponto de vista da Inteligência corporativa, uma organização pode utilizar-se de técnicas de Engenharia Social com o intuito de obter dados relevantes de seus concorrentes, explorando o comportamento humano dos funcionários da “empresa vítima” ou ainda dos seus próprios executivos.

Imagine um cenário onde uma empresa necessita obter informações à cerca do lançamento de um novo produto de seu concorrente. Para tal, ela contrata um veículo de mídia para liberar informações falsas de que seu novo produto, ainda em fase de desenvolvimento,

possuirá

uma

tecnologia

inovadora

que

sabidamente não existe. Os executivos de sua concorrente, ao terem acesso a estas informações através dos veículos de mídia, se desesperam com a possibilidade de lançarem um produto inferior no mercado e divulgam informações, até então sigilosas, sobre as novidades que seu produto virá ao mercado. Com esta ação, a empresa atacante conseguiu descobrir o que queria explorando a vaidade profissional dos executivos da empresa vítima e terá melhores condições na corrida de mercado para lançamento de produtos concorrentes.

Notem que simples ações, costumeiramente factíveis, são bons casos do uso da Engenharia Social. São inúmeros os casos de ataques de Engenharia Social que ocorrem diariamente e nós, pessoas comuns, somos potenciais vítimas de pequenos ataques envolvendo algo maior.

Existem duas categorias principais de ataques envolvendo Engenharia Social:

- Ataques com uso de tecnologia: é quando um usuário é manipulado para acreditar que está interagindo com um aplicativo ou sistema real e recebe (ou imputa) informações confidenciais através dele, tais como nomes de usuário, senhas cartões de crédito, dados de pagamento, dados pessoais, endereço e etc.

- Ataques sem uso de tecnologia: São ataques em que o engenheiro social manipula a vítima aproveitando-se de fraquezas no comportamento humano. É muito comum o agressor se passar por sequestrador e ligar para a vítima muitas vezes ao acaso, para informá-la que está em posse de um ente querido e que só irá libertá-lo após o resgate, por exemplo. Usando efeitos sonoros e persuasão, como outra pessoa se passando pelo sequestrador o agressor tenta convencer a vítima a pagar.

Nós teremos capítulos dedicados para tratar das técnicas e táticas de ataques sem uso de tecnologia, logo não iremos discorrer sobre isso com detalhes agora.

E no que tange aos ataques com uso de tecnologia, podemos citar como principais os seguintes:

Phishing

Este é talvez o ataque mais comum. Geralmente ele é realizado através de um e-mail enviado à vítima que parece ter vindo de um remetente legítimo, como por exemplo uma empresa de cartão de crédito solicitando "verificação" de informações por motivos de segurança. O e-mail geralmente contém um link para um página web fraudulenta que se assemelha com a página legítima, incluindo logotipos e conteúdo da empresa verdadeira, e contendo um formulário onde o usuário deverá informar seu login, senha, número de cartão de crédito, código de segurança e etc.

Software Interessante

Neste caso, a vítima é convencida a efetuar o download e instalar um aplicativo muito útil, como por exemplo um acelerador de desempenho da CPU, um ótimo utilitário do sistema ou um crack para um software muito caro. Neste caso, um programa malicioso como um Spyware ou um Malware (como um key logger, por exemplo) é instalado na máquina da vítima.

Mensagens de spam

E-mails, mensagens de WhatsApp e etc, que oferecem amizades,

diversão, presentes, descontos ou fotos comprometedoras de celebridades são rotineiramente enviados sob demanda com o intuito de instalar códigos maliciosos quando a vítima interage com o link ou anexo destes e-mails. No caso de um funcionário de uma empresa que execute esta ação dentro da rede de sua empresa, poderá estar colocando em risco toda a segurança da rede bem como dos dados trafegados.

Vishing

Esta é uma técnica de Engenharia Social que utiliza o telefone como vetor de ataque. Levando-se em conta a tecnologia VoIP (Voice over IP), os atacantes utilizam-se de servidores VoIP (próprios ou invadidos) para realizarem ataques de phising por telefone, através de falsificação da identificação de chamada, automação dos processos de ligação e atendimento telefônico e outros mecanismos amplamente difundidos, que podem ser implantados em computadores convencionais.

Um ataque de Vishing geralmente é deflagrado tendo como objetivo a obtenção de dados financeiros da vítima, tais como cartões de crédito, senhas de banco, etc.

Spear Phishing

Este é um conceito relativamente novo no mercado do cibercrime.

De acordo com os pesquisadores da Kaspersky, uma das maiores distribuidoras de softwares antivírus do mundo, Spear phishing é um golpe de e-mail direcionado com o objetivo único de obter acesso não autorizado aos dados sigilosos. Diferente dos golpes de phishing, que realizam ataques amplos e dispersos, o spear phishing foca em um grupo ou organização específicos. A intenção é roubar propriedade intelectual, dados financeiros, segredos comerciais ou militares e outros dados confidenciais.

Ele funciona da seguinte maneira: um e-mail é recebido, aparentemente de uma fonte confiável, mas ele leva o destinatário a um site falso cheio de malware. Esses e-mails costumam usar táticas inteligentes para chamar a atenção das vítimas. Por exemplo, o FBI alertou sobre golpes de spear phishing, nos quais os e-mails pareciam ser do National Center for Missing and Exploited Children.

Muitas vezes, hacktivistas patrocinados pelo governo estão por trás desses ataques. Os criminosos virtuais fazem o mesmo com a intenção de revender dados confidenciais para governos e empresas privadas.

Esses criminosos virtuais utilizam abordagens criadas individualmente e técnicas de engenharia social para personalizar mensagens e sites com eficiência. Como consequência, mesmo alvos do alto escalão dentro das organizações, como altos executivos, podem abrir e-mails que acreditavam ser seguros. Esse deslize permite que os criminosos virtuais roubem os dados necessários para atacar suas redes.

Pharming

Assim como o Spear Phishing, o Pharming é um novo conceito que tem ganho notoriedade na internet e dos ataques de Engenharia Social este é sem dúvidas o que mais se utiliza de tecnologia. Nele o atacante "envenena" um sistema de DNS (geralmente o ataque é realizado contra roteadores caseiros, onde o atacante consegue

acesso ao DNS interno dos roteadores e cria entradas falsas nele) fazendo com que o usuário que deseja acessar uma URL válida receba uma cópia do site desejado através de outro servidor que não seja o verdadeiro (em um ambiente de hospedagem controlado pelo atacante). Neste ponto a vítima tem certeza de estar acessando um site legítimo e acaba enviando dados pessoais, como logins, senhas e dados financeiros.

Baiting

Por meio dessa técnica, atacantes deixam à disposição do usuário um dispositivo infectado com malware, como um pendrive ou um CD.

A intenção é despertar a curiosidade do indivíduo para que insira o dispositivo em uma máquina a fim de checar seu conteúdo.

O sucesso dos ataques de baiting depende de três ações do indivíduo: encontrar o dispositivo, abrir seu conteúdo e instalar o malware sem perceber. Uma vez instalado, o malware permite que o atacante tenha acesso aos sistemas da vítima.

Pretexting

Por meio do pretexting, os atacantes fabricam falsas circunstâncias para coagir a vítima a oferecer acesso a informações e sistemas críticos. Nesse caso, os atacantes assumem uma nova identidade ou papel para fingir que são alguém de confiança da vítima. Casos icônicos de pretexting são os golpes onde atacantes se passam por funcionários de bancos e tentam obter dados de cartões das vítimas.

Tudo que o atacante precisa é dar uma olhada nos perfis das vítimas

nas redes sociais para descobrir informações como data e local de nascimento, empresa, cargo, nomes de parentes, colegas de trabalho, amigos, entre outros, e enviar um e-mail à vítima fingindo a necessidade de confirmar dados para garantir seu acesso a algum sistema específico.

Quid pro quo

Um ataque de quid pro quo ocorre quando um atacante requer informações privadas de alguém em troca de algo. “Quid pro quo”

basicamente significa “isso por aquilo”, em que o cibercriminoso oferece algo à vítima em troca de informações sensíveis.

A tática mais comum é se passar por alguém de TI e alcançar várias vítimas para encontrar alguém com um problema real de TI.

Seguindo as instruções do invasor a vítima concede acesso ao código desativa programas importantes e instala malware pensando que isso resolverá seu problema.

Outra tática bastante utilizada é simular uma investigação em que funcionários repassam uma série de informações sigilosas em troca de presentes como canetas e canecas.

Tailgating

Esta técnica é uma engenharia física e social que ocorre quando pessoas não autorizadas seguem pessoas autorizadas para locais seguros. O objetivo é obter ativos valiosos e informações confidenciais.

É o caso por exemplo quando alguém pede para a outra pessoa

"segurar a porta" porque esqueceu o cartão de acesso ou empresta seu smartphone ou computador para fazer "algo rápido" mas na verdade instala malware e rouba dados do máquina.

“A informação representa a inteligência competitiva dos negócios e é reconhecida como ativo crítico para a continuidade operacional da empresa.” (PEIXOTO, 2006).

As pessoas são um dos fatores mais importantes na segurança da informação e estão diretamente ligadas às informações à medida que participam dos processos de negócios, de modo que cada indivíduo desempenha um papel importante na manutenção da segurança da

informação.

As organizações devem se esforçar para garantir que os colaboradores entendam claramente suas responsabilidades com relação à segurança da informação, com intuito de garantir a confidencialidade, integridade e disponibilidade das informações.

(CASACA, 2014).

Os invasores podem ou não estar vinculados a uma organização.

Há também casos especiais em que colaboradores que foram desconectados da organização ainda podem representar uma forte ameaça à segurança da informação pois conhecem os processos e sistemas da empresa. As pessoas que permanecem ligadas à organização podem divulgar informações confidenciais ao público por diversos motivos, seja para ganho financeiro, insatisfação entre outros. Nas organizações as pessoas podem ser encontradas em todos os registros, por isso é importante para a segurança da informação dar atenção especial a quem tem acesso aos processos organizacionais da organização.

De acordo com MITNIK (2006), grande parte das informações aparentemente inócuas de uma empresa são cobiçadas por um engenheiro social, pois elas podem ter um papel vital em seu esforço de se revestir de credibilidade. Em sua obra Mitnik dá vários exemplos reais de ações de Engenharia Social e afirma que o grande trunfo de um atacante é ganhar acesso à informações que um colaborador de uma empresa trata como inofensivas, quando na verdade não o são.

Como vimos anteriormente, um ataque de Engenharia Social sempre terá como alvo um ativo humano, independente de cargo, posição e hierarquia. Vimos também que estes ataques são como

“jogos de quebra-cabeça”, onde o atacante reúne pedaços da informação (peças) com o intuito de ganhar credibilidade nos próximos ataques e aí sim obter os dados desejados. Porém qual seria a forma mais eficaz de proteção contra estes tipos de ataque?

Uma política de segurança bem desenvolvida, combinada a educação e treinamentos adequados, aumenta bastante a consciência do colaborador sobre o tratamento correto das informações comerciais corporativas. Uma política de classificação de dados ajuda a implementar os controles adequados para divulgação de informações. Sem essa política, todas as informações internas devem ser consideradas confidenciais, a menos que seja especificado o contrário.

Outro fato importante é que o treinamento de segurança relacionado à política da empresa criada para proteger os ativos de informação deve ser aplicado a todos que trabalham na empresa, e não somente aos times técnicos. Este treinamento deve enfatizar que, quando estiver em dúvida, o colaborador precisa verificar exaustivamente até ter certeza de que aquela pessoa pode ter acesso ao dados solicitados, mesmo que esse pareça ser inócuo do ponto de vista do mesmo.

É preciso entender também que o acesso a informação vem sofrendo gradativas mudanças com o avanço tecnológico. Em tempos antigos a grande maioria dos colaboradores não tinham acesso a informação como um todo, necessitando apenas saber da sua parte dentro do escopo completo. Por exemplo, em uma montadora de automóveis, determinado funcionário sabia que precisava colocar a peça X na posição Y e apertar os parafusos 307 e 309, e nada mais.

Com o avanço dos sistemas de informação, os funcionários precisaram ter acesso aos sistemas da empresa e entender mais a fundo do funcionamento da mesma.

Por este motivo a política de segurança de uma empresa precisa ser estendida a toda empresa, independentemente da posição. Todos devem entender que não são apenas os executivos e gestores que tem as informações que um atacante pode estar procurando. Hoje em dia, colaboradores em todos os níveis, até mesmo aqueles que não usam computadores em seu dia-a-dia, podem ser alvos.

Programação Neurolinguística

Nos capítulos anteriores nós iniciamos nossa jornada pelo estudo da Inteligência e Contrainteligência, definindo seus conceitos e objetivos e apresentando os aspectos que norteiam o tema. Adiante aprofundamos nossos conhecimentos na arte da Engenharia Social, onde além das técnicas de ataque, conversamos um pouco sobre as formas de se prevenir contra engenheiros sociais.

Neste capítulo nós iremos descer um pouco mais neste oceano de possibilidades e seremos apresentados a um novo tema, muito importante para os profissionais de Segurança da Informação que necessitarão de conhecimentos sólidos sobre Inteligência: iremos falar sobre o processo de coleta de informações protegidas, ou seja, aquelas que não estarão disponíveis de forma aberta, através da Neurolinguística.

Como já explicamos, a diferença básica entre Inteligência e

Contrainteligência é que a primeira foca na obtenção de informações relevantes para nosso modelo de negócios, tanto em fontes abertas quanto através da obtenção de dados protegidos. Enquanto que a segunda é a matéria responsável por proteger as nossas informações e dados sensíveis frente aos nossos oponentes, criando mecanismos e procedimentos que impeçam o vazamento e a divulgação não autorizada destes dados e informações.

Quando falamos de dados protegidos estamos falando de informações (sensíveis ou não) que não estão disponíveis em fontes abertas, como a internet por exemplo, e que são confidenciadas a indivíduos e/ou organizações. Um exemplo deste tipo de dado seria uma lista de fornecedores ou fabricantes, ou ainda uma carteira de clientes de uma empresa com dados de faturamento e etc. Cabe lembrar que neste ponto não discutiremos as questões morais da atividade de inteligência corporativa, haja vista que esta discussão

seria a nível de direção.

Existem diversas formas de obter estes dados protegidos, dependendo da sua aplicabilidade do meio ao qual se deseja explorar.

Neste capítulo, dando continuidade aos estudos da exploração do elo mais fraco em qualquer sistema de segurança, iremos conversar sobre as habilidades necessárias que devem ser desenvolvidas para exploração do fator humano.

Se você está lendo este livro, provavelmente já tenha ouvido o suficiente sobre PNL para deixá-lo curioso, bem como fazê-lo querer saber mais sobre seu potencial. Acima de tudo, você pode ter curiosidade sobre como as pessoas comuns a têm usado por quase 40

anos para alcançar resultados extraordinários, não só na área de Inteligência.

A PNL é uma disciplina tão abrangente que é difícil mensurar todos os seus ramos e aplicações em uma definição curta. Porém, talvez inicialmente possamos chamá-la de um conjunto de técnicas e princípios norteadores que nos permitem identificar, modelar e replicar desempenhos excepcionais em qualquer área - garantindo-nos resultados excepcionais. Usando a PNL, podemos eliminar ou modificar nossos comportamentos existentes, se não estivermos satisfeitos com eles; ou internalizar novos e mais benéficos.

Um detalhe importante que precisamos definir já no início: a PNL

não é uma “ciência oculta” ou mística que envolve, dentre outras coisas, técnicas de hipnose, etc. A PNL é baseada em princípios psicológicos sólidos, sendo nada mais do que uma forma eficaz e rápida de terapia psicológica, capaz de abordar toda a gama de desafios que provavelmente encontraremos em nossas vidas, como fobias, depressão, hábitos negativos e até mesmo desafios de aprendizagem. É uma ferramenta maravilhosa para melhorar nossa eficácia pessoal e profissional.

Enquanto a psicologia clínica tradicional trata de descrever e

analisar problemas para descobrir suas causas, a PNL foca nas possibilidades e como a mente trabalha para produzir resultados. Se a PNL pudesse ser resumida em uma frase, seria "fazer as pessoas funcionarem perfeitamente". Nossos pensamentos, sentimentos e ações específicos produziram o que somos hoje. Ao alterar essas

"entradas", você obterá resultados diferentes - um você diferente.

A PNL é uma atitude, um senso de aventura e curiosidade, um desejo de aprender que tipos de comunicação podem influenciar a nós mesmos e aos outros.

A PNL é uma metodologia baseada na ideia de que todo comportamento tem uma estrutura e um processo. Essas estruturas e processos podem ser replicados, aprendidos, ensinados e até mesmo alterados.

A PNL evoluiu para uma tecnologia inovadora, permitindo-nos organizar pensamentos, idéias e informações de maneiras que nos permitem alcançar resultados que de outra forma estariam fora de alcance.

Ao conceituar cada substantivo presente no acrônimo PLN, temos: **Programação** - a capacidade de organizar nossos sistemas neurológicos e de comunicação para atingir objetivos e resultados desejados específicos.

Neuro - o sistema nervoso por meio do qual uma nova experiência é recebida por meio de nossos cinco sentidos e processada.

Linguística - os sistemas de comunicação verbal e não verbal através dos quais as representações neurais são codificadas, ordenadas e atribuído significado.

Abaixo estão os onze princípios básicos que sustentam a PNL: **1.**

Existe uma estrutura para experimentar.

Todos nós temos padrões ou estruturas na maneira como pensamos. A capacidade de mudar o processo pelo qual experimentamos a realidade pode ser mais valiosa do que mudar o conteúdo de nossa experiência da realidade.

Por exemplo, se você gosta de Milkshake de morango, entenda o processo pelo qual você passa para chegar ao resultado do prazer.

Use esse processo em um alimento que você não gosta muito e você pode descobrir que, de repente, gosta deste determinado alimento mais do que acha. Ao mudar as estruturas, padrões e processos da maneira como pensamos, literalmente mudamos nossa experiência, o que também terá um impacto em como pensamos sobre eventos passados.

2. O significado da sua comunicação é a resposta que você obtém.

As pessoas recebem constantemente informações que são filtradas por meio de seu mapa mental interno do mundo.

A forma como você se comunica deve ser constantemente ajustada para que a mensagem que você transmite seja a que é recebida.

3. Distinções.

Todas as distinções que somos capazes de fazer em relação ao nosso ambiente, experiências e comportamento são representadas através dos nossos cinco sentidos (visão, audição, tato, olfato e paladar).

4. Já temos tudo de que precisamos - tudo de que precisamos para criar mudanças já estão dentro de nós.

A partir de nosso vasto banco de dados de pensamentos, sentimentos, memórias e sensações, podemos construir novos padrões mentais que nos permitem alcançar nossos objetivos e

sonhos.

5. O mapa não é o território.

Como seres humanos, nunca podemos conhecer a realidade.

Sempre conheceremos nossas percepções da realidade. Guarde bem este princípio pois discutiremos muito sobre ele mais a diante.

6. Nossa saúde afeta nossa mentalidade.

Nossa mentalidade afeta nossa riqueza. A negligência humana levou a questões ambientais e mudanças climáticas. Nossos pensamentos afetam constantemente nossa respiração, músculos, sistema imunológico, coração, etc., que retribuem o favor impactando nosso pensamento. Nossos corpos, nossas comunidades e até mesmo nosso universo formam um sistema complexo interdependente, todas as partes interagem e se influenciam mutuamente.

7. Não é possível isolar completamente qualquer parte do sistema do resto.

Todos os sistemas na natureza buscam naturalmente equilíbrio ou homeostase. Controle seus pensamentos, então você pode controlar sua mente, que por sua vez permite que você controle seu corpo.

8. Os comunicadores bem-sucedidos aceitam e fazem uso de toda a comunicação/comportamento disponível para eles.

Não podemos deixar de nos comunicar. Tudo sobre você -

movimentos dos olhos, linguagem corporal, tom, volume e altura de sua voz, seus hábitos e comportamentos - são todas formas de comunicação. É por isso que às vezes temos um pressentimento quando alguém está mentindo para nós.

9. Todos os resultados e comportamentos são conquistas.

Sejam eles resultados desejados ou não. Se o que você está

fazendo não está funcionando para você, faça algo diferente.

Albert Einstein descreveu a insanidade como "fazer a mesma coisa repetidamente e esperar resultados diferentes". Se você não está obtendo os resultados desejados, faça qualquer outra coisa além do que está fazendo no momento. Se você fizer o que sempre fez, obterá o que sempre obteve. Faça algo diferente, qualquer coisa, e você obterá um resultado diferente.

10. Se alguém pode fazer algo, qualquer outra pessoa também pode aprender a fazê-lo.

Quando Roger Bannister correu uma milha em menos de quatro minutos em 1954, ele foi a primeira pessoa a quebrar esse marco na história registrada. Desde então, milhares de pessoas alcançaram essa

façanha - na verdade, seu recorde ficou por apenas algumas semanas.

Se modelarmos o pensamento, o comportamento e as ações de pessoas que já tiveram sucesso em uma determinada área, poderemos alcançar resultados semelhantes.

11. Sempre fazemos as melhores escolhas disponíveis para nós.

Essas escolhas são baseadas em nossas experiências. Mais e melhores experiências permitem mais escolhas. Se você teve apenas um relacionamento e ele terminou dolorosamente, quando você conhece alguém novo, você pode inconscientemente associar um relacionamento com dor. Você pode sabotar esse relacionamento potencial para evitar a dor. Conforme você tem mais relacionamentos e começa a associá-los com diversão, amor e alegria, é provável que você faça algo diferente e mais escolhas positivas.

Praticando o PNL: Rapport e Âncora A comunicação envolve no mínimo duas pessoas interagindo uma com a outra, e as pessoas interagem por meio de uma variedade de canais e de muitas maneiras diferentes - cara a cara, no telefone, por meio de dança, internet, redes sociais, toque e assim por diante.

Para se tornar um influenciador mais eficaz você deve desenvolver a habilidade de prestar atenção em todos os detalhes de forma consciente na pessoa (ou pessoas) com as quais você está tentando se conectar.

Estes detalhes incluem, principalmente:

• Linguagem verbal (tom e variação da voz)

• Movimentos oculares

• Fisiologia (linguagem corporal)

Figura 1: Filtros comportamentais

Para muitos de nós, nossos principais métodos de comunicação são baseados em tecnologia: e-mail, mensagens de texto, Facebook, etc, os quais utilizam somente as palavras que digitamos para transmitir as nossas mensagens. Mas esta é a abordagem mais eficaz?

Quanto da comunicação são apenas palavras? A maioria das decisões são feitas com base no relacionamento!

Por exemplo: Sabia que é mais provável que você compre de alguém com quem você poderia se relacionar do que com alguém que

você não poderia? – em linhas gerais, as pessoas gostam de pessoas que são como elas mesmas.

Quando as pessoas confiam e se sentem confortáveis uns com os outros, barreiras caem e coisas interessantes acontecem: elas começam a agir como as outras, assumindo suas posturas e trejeitos

– e tudo isso, inconscientemente.

Quantas vezes você ficou surpreso com a forma de como a comunicação pode dar muito errado, e como é fácil ser interpretado de forma errada por um simples gesto que não deveria ter sido feito?

Você já se sentiu confortável e reconhecido por alguém, mesmo que esta pessoa estivesse discordando de você? Já reparou que algumas pessoas você gosta instantaneamente, enquanto outras você não consegue gostar? E quando conseguimos falar com algumas pessoas por horas que nos parecem apenas minutos?

A resposta para todas essas perguntas é o relacionamento – o processo mais importante em qualquer comunicação. E esse relacionamento, a luz da PNL, podemos traduzir como Rapport, que nada mais que é a capacidade de entrar no mundo de outra pessoa.

O Rapport é a habilidade de ver o ponto de vista do outro (não necessariamente concordar com isso), estar no mesmo comprimento de onda e apreciar os sentimentos um do outro.

Quando as pessoas estão se comunicando em harmonia é fácil de ser entendido e acreditar que suas preocupações são altamente consideradas pela outra pessoa. Em um nível inconsciente, há uma sensação confortável de: 'Esta pessoa pensa como eu, logo eu posso relaxar'.

Em outras palavras, o que quero dizer é que apenas uma pequena parte da nossa comunicação é efetivamente feita através do que nós dizemos. E quem entende este princípio passa a fazer parte do grupo de pessoas que se destacam, que motivam as outras, influenciam, negociam, lideram e conseguem capacitar as demais.

Em particular, você precisa se concentrar no resultado desejado, no propósito da sua comunicação:

• O que exatamente eu desejo alcançar?

• Como saberei que minha comunicação foi bem sucedida?

• Quais serão as evidências sensoriais do sucesso. O que eu devo ver, ouvir e sentir?

Vamos fazer um simples exercício para colocarmos em prática estes ensinamentos.

Com seu parceiro/parceira, faça uma determinada declaração verbal e tente contradizer esta afirmação com sua linguagem corporal e/ou com seu tom de voz, e perceba qual será o impacto sobre a comunicação.

Por exemplo:

1. Diga ao seu parceiro que você realmente gostou do que ele fez nos seus cabelos enquanto balança a cabeça de um lado para o outro em um gesto negativo;

2. Use palavras para comunicar ao seu parceiro que você está muito zangado por determinada situação, porém transpareça que está com muito sono, falando com calma e com um tom de voz macio; e 3. Experimente usar incongruências entre palavras, tom e linguagem corporal e observe o impacto que isto tem sobre como a comunicação é recebida por seu parceiro.

Após este exercício tente mensurar se a mensagem que foi passada verbalmente foi recebida da forma que seria recebida se todos os elementos da comunicação (linguagem verbal, movimentos dos olhos e linguagem corporal) estivessem em sintonia.

Qualquer comunicação pode ser descrita como um conjunto de quadros (frames), onde cada um depende dos quadros ou respostas anteriores. Vamos a um rápido exemplo: quando você faz uma determinada declaração, a outra parte responde a sua mensagem, e a sua escolha de palavras para o próximo quadro será então decidida considerando esta resposta. Correto?

Um outro exemplo, se você apresentar uma ideia enquanto tenta convencer alguém, o destinatário pode aceitar a ideia ou discordar dela em vários aspectos. Você precisará construir sua próxima declaração, analisando esta resposta, e escolher palavras de modo a persuadir completamente o destinatário.

Ao longo da conversa, seu objetivo é expressar a intenção e os benefícios da ideia para o destinatário, por mais absurda que possa soar para ele no início, e não importa o quão antagônico elas estariam no começo.

É importante que você sempre mantenha um nível de respeito e dignidade na escolha das palavras, para não ofender a outra pessoa, pois se você parecer muito agressivo, ele provavelmente fugirá de você.

Para usar com eficiência os padrões persuasivos de linguagem descrito na PNL, você deve compreender os melhores aspectos da comunicação entre você e seu interlocutor, bem como a função dos padrões em todo o processo - um padrão de persuasão essencialmente compreende três partes: um quadro, uma resposta e uma significação.

Uma vez que um quadro é entregue pelo mensageiro, usando palavras para descrever cuidadosamente seus pensamentos, o destinatário retornará uma resposta relacionada. Esta resposta será a chave para formular sua tréplica.

È importante balancear a conversa de forma que não só você exponha seus pensamentos e lidere o momento. Deixe seu

destinatário liderar um pouco, pois assim ele se sentirá confortável e você poderá analisá-lo da melhor forma para montar os próximos quadros com o objetivo de persuadi-lo.

O método de persuasão e influência da PNL não é um processo unilateral: acontece em ambos os lados. Enquanto você tenta influenciar um destinatário, o destinatário também está tentando influenciá-lo. Portanto, é essencial observar esses padrões de maneira ativa para que você possa dar uma resposta melhor.

Harmonia, concordância e afinidade

Quando você cria um Rapport está desenvolvendo uma compreensão da outra pessoa. Você mostra a ela que você pode identificar-se e até compartilhar sua experiências. O Rapport significa uma relação de harmonia, acordo ou afinidade. Este é o processo mais importante em qualquer interação. Sem relacionamento, você não obterá um resultado produtivo.

A primeira coisa que você nota quando vê duas pessoas juntas que realmente se dão bem é como eles são muito parecidas. Você vai notar isso principalmente quando você vê duas pessoas que se amam, juntas. Eles vão olhar nos olhos um do outro com a mesma expressão em seus rostos, eles exibirão a mesma linguagem corporal, e eles estarão falando com o mesmo tom de voz e ritmo de discurso.

Ao observar o processo pelo qual duas pessoas chegam a sentir-se mais em casa um com o outro, é possível utilizar as lições aprendidas para aprimorar esse efeito quando você está falando com outras pessoas e deseja persuadi-las.

Na maioria das vezes, criamos rapport com outras pessoas

inconscientemente e naturalmente, mas há ocasiões em que nossas maneiras intuitivas de criar rapport não funcionam, e são nestas ocasiões que precisamos recorrer a certas habilidades para criá-lo conscientemente. É aí que entra a PNL. Ela exige foco e concentração!

Criar um Rapport envolve mostrar um interesse genuíno, observar e ver como uma pessoa reage ao que você diz e identificar as palavras-chave ou frases utilizadas. O relacionamento ocorre não apenas no que você diz, mas também em suas ações e linguagem corporal, o que geralmente acontece no subconscientemente.

O processo de estabelecimento de relacionamento deve começar com o primeiro aperto de mão. Criar rapport não tem nada a ver com gostar ou ser apreciado. É uma maneira de dizer a uma pessoa: 'Nós compartilhamos um terreno comum; você será ouvido e apreciado.'

A chave para construir relacionamento é a capacidade de entrar em alguns mundos do outro corpo, assumindo um estado de espírito semelhante. A primeira coisa a perceber sobre os estados de espírito é que eles são intimamente ligados à linguagem corporal.

Se alguém está sentado com os braços e pernas cruzado e com uma carranca no rosto, você pode assumir com segurança que eles não vão ser muito receptivos ao que você tem a dizer. Se, por outro lado, eles têm uma postura aberta (ou seja, braços e pernas em posições abertas, razoavelmente relaxadas), então eles vão ser mais abertos ao que você tem a dizer.

Você já percebeu que quando você se sente deprimido você tende a ficar com a cabeça baixa, arrastando seus pés? Tente se sentir deprimido enquanto pula e sorrindo - você descobrirá que não é possível. É importante lembrar-se de que seu estado emocional está intimamente ligado ao seu Estado físico.

Em outras palavras, se você deseja criar relacionamento com alguém, basta que você tente entrar no mundo dele, e depois você poderá ver as coisas da perspectiva dele, sentir como ele se sente e, a partir daí, aprimorar toda a relação.

O processo pelo qual você entra no mundo de outra pessoa é chamado de espelhamento. A tecnologia de espelhamento foi criada por Milton Erickson no início 1970 em seu trabalho com hipnoterapia

clínica.

O espelhamento é basicamente copiar o corpo da outra pessoa com

linguagem, respiração e padrões de voz para se tornarem como eles. Está literalmente se tornando uma imagem espelhada da outra pessoa. Quando você fizer isso, vocês dois sentirão como se conhecessem desde sempre.

Parece um pouco difícil de acreditar primeiro, mas depois de experimentar, você verá por si mesmo como é verdade.

Algumas pessoas acham a ideia de espelhamento desconfortável e sentem que estão tentando enganar ou tirar vantagem da outra pessoa, mas o espelhamento ocorre naturalmente como parte de construção do rapport, então não sinta que está fazendo nada falso.

Tudo o que você está fazendo é estar ciente desse processo para tentar melhorá-lo. E de qualquer maneira, se você se sentir mal por fazer isso, então você provavelmente não é o tipo de pessoa que tira vantagem de qualquer pessoa - então não se preocupe.

Comece alinhando sua linguagem corporal. Tente não fazer isso de forma muito óbvia, ou vai parecer que você está zombando da outra pessoa, e isso naturalmente terá o efeito oposto.

Olhe para as coisas com o mesmo ângulo de cabeça que seu interlocutor, mantenha suas pernas numa posição muito semelhante as dele, se ele estiver de pé, fique também. Se os braços dele estão cruzados, com naturalidade, cruze os seus. Repare na sua expressão facial e tente reproduzi-la. Ou seja, copie sutilmente a postura dele e você sentirá a mudança de interação dele contigo.

Você pode tentar espelhar alguém pela metade, se sentir desconfortável com o espelhamento total no início. Para meio-espelho, simplesmente faça uma meia versão do que a outra pessoa está fazendo. Por exemplo, se ele cruzar seus braços, você pode segurar um dos cotovelos com a outra mão.

Se ele têm as mãos nos bolsos, você pode colocar uma mão no bolso. Se ele está balançando para frente e para trás com seus pés, você pode balançar de vez em quando. Basta copiar a linguagem do corpo dele ao ponto que você se sinta confortável.

Ouça o ritmo e o tom da voz da outra pessoa. E se ele estiver falando rápido, então você deve falar rápido também. Se a pessoa usa pausas em suas frases, então você deve tentar para corresponder a esse padrão de fala. Esteja atento e você será capaz de aprender muito mais trejeitos (e muitos deles sutis) do que você está acostumado.

Lembra dos princípios norteadores do PNL? Obviamente que todos são importantes, mas na minha concepção um dos principais é, sem dúvida, o princípio 5 – O mapa não é o território. Ele nos fala que somente nós conseguimos conhecer a nossa percepção da realidade, ou seja, é o nosso estado mental perante a verdade.

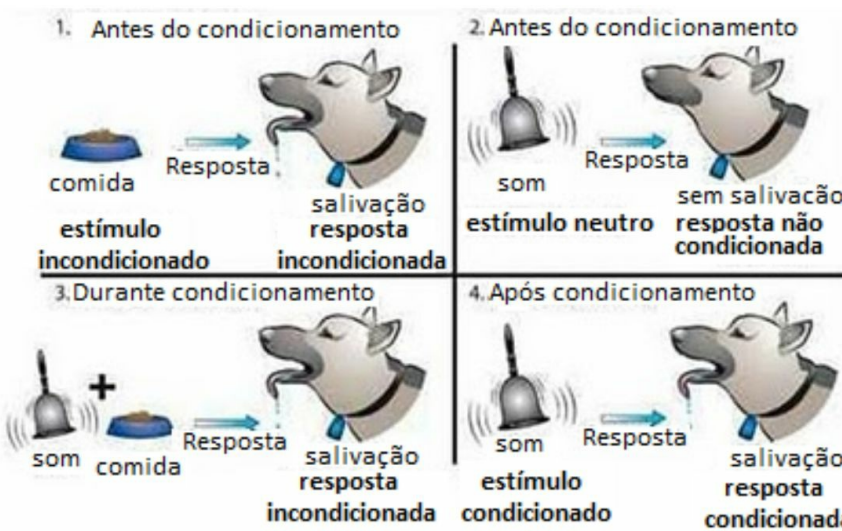
Âncoras

Uma âncora é um estímulo que nos lembra de determinados eventos e podem mudar o nosso estado positiva ou negativamente.

Portanto, são muito potentes, porque nos dão acesso instantâneo a estados de grande força, ou grande fraqueza.

Conforme ALLEN (2018) esses estímulos podem envolver todos os sentidos e podem ser internos e externos. Toda âncora é uma associação que se cria entre os pensamentos, as ideias, as sensações ou os estados e um determinado estímulo.

Um exemplo clássico de âncora é o experimento do Doutor Ivan Pavlov, que deixava carne próxima de cães famintos, e estes começavam a salivar ao perceber esse poderoso estímulo, e quando se achavam nesse estado de salivação intensa, Pavlov fazia soar uma campainha. Em pouco tempo, deixou de ser necessária a carne para produzir a salivação, ou seja, bastava os cães ouvirem a campainha e começavam o processo tal como se tivesse sentido o cheiro da carne.



Desta forma, Pavlov criou em seus cães um vínculo neurológico entre o som da campainha, as sensações de fome e o reflexo de salivação.

Figura 2: Experimento “O Cão de Pavalov”

Conforme ALLEN (2018), vivemos em um mundo cheio de situações de estímulos e respostas, de modo que grande parte do comportamento humano consiste em respostas programadas, inconscientemente, por exemplo, sob condições de tensão, algumas pessoas apelam automaticamente ao cigarro, ao álcool ou até mesmo as drogas. A chave do que você está lendo neste momento está em que toma a consciência deste processo, de forma que, se as âncoras existentes em você ou nos outros, não são úteis, podem ser eliminados e substituídos por novos vínculos estímulo-resposta. Você pode pensar em algumas situações nas quais gostaria de criar âncoras

nas pessoas, para gerar uma resposta específica, por meio de um estímulo proposto? Muito bem, então, você vai aprender como se criam as âncoras.

Sempre que uma pessoa está em um estado intenso e, sob estas condições, lhe é fornecido simultaneamente, um determinado estímulo que coincida com o momento culminante deste estímulo, se criará entre ele e o estímulo um vínculo neurológico, da mesma forma que aconteceu com os cães de Pavlov. Desta forma, cada vez que aparecer este estímulo no futuro, irá gerar o mesmo estado intenso de forma automática.

Ao analisarmos as técnicas de PNL vemos que nem sempre em nossas relações diárias as pessoas estão sendo elas mesmas conosco (inclusive nós, ao realizarmos uma ação de Engenharia Social, não estamos sendo nós mesmos). E isso nos remete a uma frase que costumeiramente falo aos meus alunos: o mundo é cinza. Para a Inteligência (e infelizmente, as vezes, para a vida) não existe o preto ou branco, o certo ou errado, o moral ou imoral… todos estão atuando em um dos seus papéis com um propósito específico. Você não concorda? Pense por um instante: você age no seu trabalho da forma que age em casa? Você se relaciona com seu gestor como se relaciona com seu filho? Não, não é mesmo? E por que isso?

Justamente pois nós inconscientemente assumimos papéis em nosso dia-a-dia para algum propósito específico.

Eu sei que pode parecer estranho no início, mas ao nos depararmos com essa verdade, e analisarmos essa concepção de forma mais macro nas nossas vidas, vemos que estamos corriqueiramente tentando passar uma imagem que não condiz com 100% da verdade, em outras

palavras, estamos influenciando as pessoas com as quais interagimos para que tenham as suas percepções perante a verdade, ou melhor dizendo, estamos manipulando-as para que tenham as percepções que desejamos.

Técnicas de Argumentação e

Convencimento

Neste capítulo veremos os princípios gerais de persuasão, a arte da argumentação e do convencimento, os quais aplicados com as técnicas de Programação Neurolinguística, se tornarão uma poderosa ferramenta para aumentar suas habilidades de persuasão.

Quando falamos em influência e persuasão, um dos melhores especialistas do mundo é Robert Cialdini. Ele foi Professor de Psicologia e Marketing da Universidade do Arizona, nos EUA, e ficou famoso após o seu Best-Seller “As Armas da Persuasão”.

Depois de décadas de pesquisas e estudos, Cialdini identificou as principais áreas de influência e as sintetizou em 5 princípios, os quais nos ensinam como podemos facilmente influenciar os outros.

Vejamos:

a) Princípio 1: Reciprocidade

Nós evoluímos para ser criaturas sociais, e como resultado, as pessoas tendem a retribuir favores. Se alguém realiza alguma ação útil para com o outro, este sentirá a necessidade instintiva de

"retribuir" esse favor.

Um exemplo do uso do princípio de reciprocidade são os Hare Krishna. Quando você visita alguma região que possui templos Hare Krishna, é comum vermos discípulos na localidade abordando as pessoas na rua. A técnica deles é simples: eles te dão algum objeto e dizem que é um presente. No entanto, uma vez que o "presente" for aceito, o discípulo pedirá uma contribuição. Essa técnica é fantástica pois vem aumentando o número de doações que eles recebem.

b) Princípio 2: Compromisso e consistência

Comprometer-se com uma meta ou ideia, seja escrita ou verbal, aumenta muito a probabilidade da pessoa honrar o compromisso, mesmo que não haja incentivo para fazê-lo ou se o motivo original for

excluído após o término do acordo. A razão por trás desse princípio é que o apego nos faz querer estar em harmonia com nossa auto-imagem.

c) Princípio 3: Prova social

Imagine que você está dirigindo em uma cidade onde nunca esteve e de repente vem aquela fome. Você repara que há somente dois restaurantes nesta cidade: um bem grande, com uma fila enorme, e outro praticamente deserto. Qual deles você escolheria?

9 de cada 10 casos iriam para o que está cheio, simplesmente pelo fato de “estar cheio”. Inconscientemente temos a certeza de que, se todos os outros estão lá, este deve ser o melhor restaurante. Esse é um exemplo claro da prova social.

Outro exemplo bem comum do uso desta técnica são em campanhas de marketing do tipo "Junte-se aos outros 300.000

membros felizes" ou "Usado por milhões de clientes satisfeitos".

Inconscientemente isso gera nas outras pessoas o senso de que, se tem muitos membros, é bom e eu deveria estar lá também.

d) Princípio 4: Autoridade

As pessoas tendem a obedecer a figuras de autoridade mesmo quando são solicitadas a fazer algo questionável, ou como alguns estudos mostraram, completamente antiético.

Um exemplo prático deste princípio que vemos claramente na história da humanidade, foi na II Guerra Mundial, mais especificamente, no julgamento do Nuremberg, onde os oficiais Nazistas foram interrogados no pós-guerra.

Muitos deles alegaram que, mesmo não concordando com as ordens de Hitler, as quais levaram a execução dos mais de 6 milhões de Judeus, cometiam as atrocidades sem questionar simplesmente por

estarem seguindo uma ordem.

e) Princípio 5: Gostar

As pessoas são mais propensas a ser influenciadas ou persuadidas, pelas pessoas de quem gostam ou que admiram.

Este princípio é um tanto quanto óbvio hoje em dia, pois vivemos

cada vez mais imergidos em um mundo baseado na influência digital.

Independente da plataforma, sejam YouTubers, Instagramers, TikTokers ou qualquer outra coisa, as pessoas vem sendo facilmente influenciadas por completos desconhecidos, os quais anulam suas vidas pessoais para fazerem parecer viver “em um conto de fadas” –

uma vida perfeita. E obviamente, pelo princípio da Prova Social como vimos anteriormente, as pessoas tendem a seguir e imitar seus

“ídolos”, justificando-se pela simples desculpa de “está na moda”.

O grande objetivo de aprender sobre este princípios de influência é que eles nos permitem explorar as três necessidades básicas do ser humano. E entendê-las, aliado a todas as técnicas anteriores que vimos até aqui, nos permite dominar a arte de influenciar e convencer as pessoas. Vejamos:

a) Necessidade de afiliação

Os seres humanos são, em sua essência, sociais e querem se sentir amados. A rejeição não agrada a ninguém, e faremos de tudo para evitá-la.

A psicologia explica que desde o nosso nascimento nós aprendemos que fazemos parte de grupos sociais. Quando o bebê entende que ele e a mãe não são mais um, ele começa a reparar que faz parte de uma família. Ao final da infância, perto da puberdade, o indivíduo começa a sentir a necessidade da independência do seu ninho, porém ao invés de simplesmente deixá-lo para viver uma vida solo, ele procura outro grupo que o aceite através das suas afinidades comuns, as quais podem ser gostos musicais, esporte praticado,

hobbies e etc, e assim passamos a nossa adolescência. Não obstante de tudo que já vivemos, na fase adulta é exatamente igual: sempre temos a necessidade de nos sentirmos aceitos em um grupo social, e é por isso que temos alguns desvios de carácter extremos, como por exemplo pessoas que não tem personalidade (querem tanto serem aceitas que absorvem a personalidade do grupo que deseja fazer parte), ou as que não conseguem se enturmar de forma alguma.

Chegando, infelizmente, a extremos como o suicídio.

b) Necessidade de estar certo

Para atingir nossos ideais em um mundo complexo devemos nos

esforçar constantemente para encontrar o melhor caminho para os nossos objetivos. Temos a necessidade de estar certos, nossas relações sociais como por exemplo a forma de tratar um gestor, ou ainda a necessidade de tomar a decisão certa em um relacionamento amoroso. Independentemente da situação, as pessoas sempre têm dificuldade em encontrar a resposta “certa”, mas sentem a necessidade de afirmar pra si mesmo que tomaram a decisão certa.

Os influenciadores entendem essa necessidade e se esforçam para criar coisas que nos façam sentir saciados desta necessidade. Por exemplo, autoridades exercem uma grande influência sobre as pessoas porque oferecem um ponto de vista ou maneira "correta" de fazer as coisas, especialmente uma maneira de fazer as coisas sem que pensemos muito. As técnicas de teste social apelam aos nossos desejos precisamente porque achamos que os outros podem estar certos e não queremos sentir que “perdemos”.

c) Necessidade de Poder

Todo ser humano tem a necessidade de sentir que é o “ser dominante”. Claro que o grau de influência desta necessidade varia muito em cada tipo de pessoa, porém é senso comum que o nosso ego precisa ser afagado.

Um exemplo claro disso é na infância, quando passamos por

aquela fase do egoísmo. “Isso é meu!” ou “Ele pegou o meu brinquedo, não vou emprestar” são frases que ninguém ensina mas as crianças já sabem muito bem falar. E nós crescemos com esse senso de que precisamos estar no comando de algo, seja da nossa vida, das nossas escolhas ou até, nos casos extremos, da vida alheia.

Essa necessidade é tão nociva que, mesmo pessoas que nunca se imaginaram na posição de dominadoras ou usurpadoras, quando sentem o “gostinho do poder”, deturpam o seu carácter e realizam ações pelas quais chegamos a desconhecer o indivíduo de tão antagônicas com sua personalidade elas podem ser.

Bom, até aqui nós vimos os princípios de influência e as necessidades básicas que cada pessoa busca satisfazer, e agora chegou a hora de entendermos como podemos estruturar a nossa mensagem (ou forma de comunicação) para persuadirmos nossos interlocutores.

As regras da comunicação bem sucedida

A depender do autor que você consulte, existem muitas regras para

uma comunicação bem sucedida. No entanto, como nosso objetivo é lhe dar ferramentas práticas para ações pontuais, citaremos três regras fundamentais:

a) Simplicidade

A linguagem mais eficaz lança luz em vez de deixar dúvidas.

Quanto mais simples uma ideia, mais fácil será de entender e portanto mais crível ela será. O princípio da simplicidade rege quase todas as áreas de nossas vidas. Não é a toa que a cultura minimalista tem tomado conta do senso comum.

Se formos analisar nossas interações na internet, a maioria das pessoas se comunica através de emojis e/ou figurinhas do WhatsApp ao invés de escreverem textos mais longos. Portanto, se você está prestes a transmitir uma mensagem importante, seja o mais breve possível. Nunca use um parágrafo quando uma frase é suficiente.

Nunca use quatro palavras quando três poderiam dizer o mesmo.

b) Repetição

Quando falamos de repetição temos vários exemplos práticos que poderíamos utilizar para apresentar esta regra, porém como comentamos no início deste livro sobre a influência militar na área de Inteligência, vamos entender essa regra do ponto de vista do sistema de ensino militar.

Em um curso de formação militar básica (seja ele qual for) é muito comum utilizar a regra da repetição com o intuito de aumentar o coeficiente de aprendizagem dos alunos. Desde instruções simples, como a Ordem Unida (comumente conhecida como os desfiles militares), até instruções mais avançadas, como nos cursos de formação Paraquedista, a repetição é o carro chefe. E os alunos ficam horas, dias e semanas repetindo os mesmos movimentos com o intuito de gerar memória muscular.

Em uma comunicação persuasiva, submeter o interlocutor em um cenário onde se crie um sistema de repetição (seja de palavras e/ou gestos) fará com que ele absorva aquela informação de forma insconsciente, potencializando o poder de influência.

b) Credibilidade

Abraham Lincoln dizia, "Não se pode enganar todas as pessoas todo o

tempo". Se suas palavras carecem de sinceridade, contradizem fatos, circunstâncias ou percepções, você perde a credibilidade.

Na vida poucas coisas valem mais do que a nossa reputação. Isso não é verdade apenas para a classe política, também é verdade para você e eu. A publicidade excessiva aliada a um discurso falso, pode ser um jogo extremamente perigoso. Mas como ganhar credibilidade?

É muito simples. Deixe as pessoas saberem quem você é e o que você faz, então torne-se essa pessoa, faça o que você disse que faria. E

finalmente: lembre-os de que você é o que disse que seria.

Esta regra é incrível se analisada a luz da PNL e do Rapport!

Se o influenciador entender que ele consegue manipular o estado da mente do interlocutor frente a verdade e conseguir estabelecer um Rapport, será muito mais fácil dar credibilidade, ou sustentar, uma

“Estória de Cobertura”. Esta técnica é muito utilizada nos meios de Inteligência para que o agente assuma papéis e consiga convencer seus alvos de que ele é quem alega ser.

Um exemplo bem interessante do uso desta técnica, e desta vez fora dos meios militares, é o “Caso do filho do dono da Gol”. Marcelo Nascimento da Rocha era uma pessoa comum, apesar de ser um

“mentiroso nato”.

Após passar sua vida aplicando golpes ao se passar por pessoas que não era, ele um dia decide se passar pelo filho do dono da companhia aérea Gol. O golpe foi tão bem feito e sustentando que ele chegou a ser entrevistado em programas de celebridades, realizou viagens e “alugou” camarotes em festas de alta sociedade, somente através da sua forma de comunicação persuasiva.

O caso foi tão emblemático que virou filme na Netflix – “Vips: histórias reais de um mentiroso”.

O efeito Benjamin Franklin

O Efeito Benjamin Franklin tira proveito de um fenômeno bastante contra-intuitivo. Em suas próprias palavras ele descreveu assim: "A pessoa que te fez favores estaria mais disposta a fazer qualquer coisa por você do que aquela que você ajudou".

Esse fenômeno é causado por "dissonância cognitiva" o que significa que nossos cérebros têm problemas com duas ideias opostas.

No caso do efeito Benjamin Franklin essas duas opiniões opostas seriam "eu não gosto dessa pessoa" e "eu ajudei essa pessoa" por

isso, o cérebro, lutando com estas duas ideias contraditórias, defende que ajudamos as pessoas que gostamos e não fazemos favores para as pessoas que não gostamos, não é verdade?

Em sua autobiografia Franklin discute a aplicação desse método à hostilidade de um legislador rival: "Tendo ouvido que tinha em sua biblioteca um certo livro muito escasso e curioso, escrevi uma nota, expressando a ele a minha vontade de ler esse livro e pedindo-lhe que me fizesse o favor de emprestá-lo por alguns dias. Ele me enviou de imediato e devolvi para ele cerca de uma semana com outra nota, expressando forte agradecimento ao favor. Quando nos encontramos na Câmara, falou comigo (e nunca tinha feito isso antes) muito cortês e manifestou sua disposição em me servir em todas as ocasiões, de modo que nos tornamos grandes amigos, e a nossa amizade continuou até sua morte."

Então a lição a ser aprendida é a seguinte: se você quer se dar bem com alguém é melhor pedir que façam algo por você (por menor que seja) do que fazer algo por ele.

Fundamentos da Anonimização

Até aqui nos aprofundamos nas técnicas de manipulação do fator humano. Vimos como utilizar a PNL para analisarmos o nosso interlocutor, como usar o Rapport pra “entrarmos em seu mundo” e principalmente, vimos nas técnicas de persuasão, como manipular a comunicação ao nosso favor. E daqui por diante mergulharemos nas técnicas que envolvem o uso da tecnologia para nos auxiliar nas ações de OPSEC.

Nos primórdios da internet a privacidade dos usuários era algo comum, na realidade não se pensava em outra forma de se utilizar a Rede Mundial. Nesta época os primeiros fóruns e salas de bate-papo, por exemplo, não cobravam dos usuários seus dados básicos de acesso, tais como endereço IP, tipo de navegador e sistema operacional e etc. Porém através do fomento do uso das publicidades massivas na Rede, percebeu-se o poder que mecanismos de identificação dos usuários, tais como os cookies, teriam para potencializar as publicidades direcionadas. Quem nunca ouviu a expressão “Na internet, se você não

consome um produto você é o produto”?

E neste escopo caótico de abusos de privacidade, trabalhar como Analista de Inteligência ou realizar ações OPSEC pode ser uma tarefa um tanto arriscada, uma vez que, manter-se anônimo na Rede não é uma tarefa trivial.

Por que Anonimizar?

Do ponto de vista de OPSEC, um profissional de Cyber Security nunca pode se revelar no ciberespaço, haja vista que muita das vezes este estará realizando ações de caráter investigativo e/ou explorativo.

E ter sua real identidade, bem como sua origem (endereço IP, User Agent do browser, Sistema Operacional e etc) disponíveis para seu alvo poderá levá-lo a sérios problemas.

Imagine um cenário onde você, integrante de um Red Team da empresa XPTO, recebe a tarefa de explorar vulnerabilidades do site de uma filial da sua empresa, sem que o time de segurança desta saiba que estão sendo testados, pois este teste será realizado para identificar, além de brechas de segurança, a execução do trabalho de proteção cibernética que este time deveria estar realizando nos ativos.

Dentro deste escopo não basta ser um exímio Pentester se não souber realizar uma anonimização adequada, pois o sucesso da tarefa depende primordialmente de não ser descoberto.

De posse dos conceitos até agora abordados poderíamos então inferir que anonimizar seria estar indetectável no mundo cibernético?

Não. A Anonimização consiste em dificultar a autoria de um determinado tráfego de dados. Ela é a “kriptonita” do Analista de Incidentes de Rede, pois o objetivo do trabalho deste é, basicamente, identificar o autor de um evento ou incidente cibernético. No entanto, através da anonimização esta identificação torna-se difícil de ser confirmada, levando o Analista de Incidentes a inferir baseado em erros, de forma que o real autor das ações quase sempre não é descoberto.

Identificando a origem do tráfego

Antes de falarmos especificamente das técnicas de anonimização, precisamos estabelecer alguns fundamentos importantes.

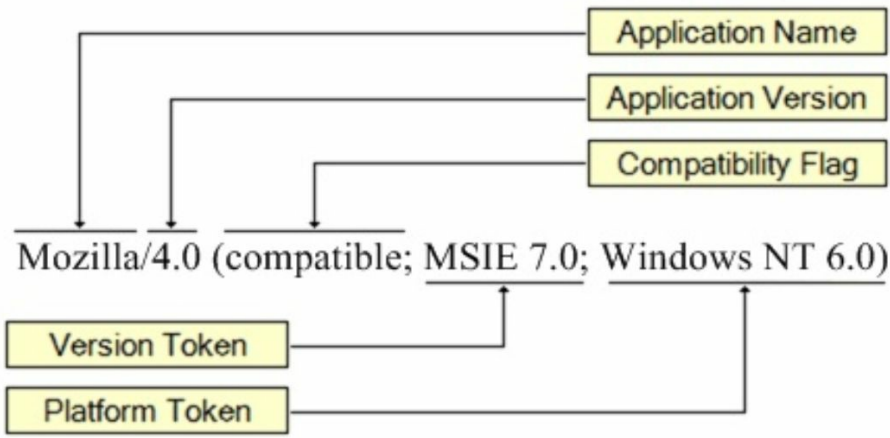
Existem algumas formas de garantir a autoria de uma ação

cibernética. Uma delas é através do Fingerprint (que trataremos em um capítulo dedicado, mais a frente) e as outras se baseiam no uso de algumas tecnologias, como por exemplo:

a) IP

A Rede Mundial de Computadores é baseada em protocolo TCP/IP

e as faixas de IP disponíveis e seus respectivos donos (ou responsáveis) são gerenciados pela IANA (Internet Assigned Numbers



Authority). Logo o IP que seu ISP (Internet Service Provider) lhe disponibilizou (mesmo que de forma dinâmica) é de conhecimento do mundo todo. Não só ele mas os dados relativos a ele também, tais como origem, nome do ISP e DNS. Desta forma, realizar uma ação cibernética utilizando seu IP real não é uma boa coisa.

b) User-Agent

Quando solicitamos uma página Web, o nosso browser envia uma série de cabeçalhos para o servidor. Cada cabeçalho contém detalhes que ajudam o servidor a determinar a melhor maneira de fornecer a informação solicitada. A sequência do User-Agent pode conter detalhes opcionais chamados tokens, que devem ser colocados entre parênteses e que variam entre os diferentes programas.

A figura abaixo mostra de forma bem didática um exemplo de um User-Agent enviado pelo finado Internet Explorer, a qual destaca os tokens.

Figura 3: User-Agent

A string User-Agent contêm 3 tokens:

- A flag Compatibility é usado pela maioria dos browsers mais modernos. Ela indica que o navegador é compatível com um conjunto comum de características.

- O token Version identifica o browser e contém o número da versão. A versão do token no exemplo (“MSIE 7.0”) identifica o Internet Explorer 7.

- O token Platform identifica o sistema operacional e contém o número da versão. O token Platform no exemplo (“Windows NT 6.0”) indica o Windows Vista.

Desta forma, compartilhar seu User-Agent verdadeiro com o alvo não é uma boa opção, pois dados importantes estão sendo expostos.

c) Cookies

Os cookies são pequenos arquivos armazenados temporariamente nos navegadores e que compartilham o que o internauta está visitando na rede. Não há limite para quais informações os cookies podem armazenar, podendo ser desde um endereço de e-mail, as preferências de pesquisa no Google, a cidade de onde você está conectado, os sites que você visitou anteriormente, credenciais de acesso a um determinado site, contas de Redes Sociais e e-mail que esteja logado no momento do acesso e muito mais. E é justamente essa capacidade de registro que pode tornar o cookie um grande vilão.

d) Geolocalização

Muitos sites atualmente utilizam a localização do usuário para lhe fornecer conteúdo personalizado e alguns navegadores modernos e sistemas operacionais já fornecem isso aos sites mesmo que você não autorize.

Quando falamos em anonimização, a geolocalização é um ponto crucial de cuidado pois ela pode colocar a perder todo cuidado prévio que o analista teve de ofuscar seu IP, dentre outras informações.

d) Correlação de tráfego

Apesar de ser subjetiva, a correlação de tráfego é amplamente utilizada por analistas de incidentes de rede para tentar identificar acessos anonimizados.

Imagine que você necessita realizar alguma ação em determinado site e, antes de realizá-la, decide visitar o site para testar suas funcionalidades. Porém durante os testes você identifica uma possível vulnerabilidade em determinada página e decide atacar. A partir deste momento você utiliza as técnicas de anonimização para realizar sua ação e, após realizá-la, você "desanonimiza" sua conexão e acessa novamente o site para ver se a sua ação teve êxito.

Até aí tudo ok, certo? Não. Dado ao fato de você ter realizado acessos legítimos enviando seu fingerprint e as informações das tecnologias usadas para acessar o referido site, antes e depois do ataque, o analista de incidentes consegue identificar você como o possível atacante.

Se escondendo na Rede

Até agora aprendemos como somos conhecidos na internet porém o que devemos fazer para não sermos identificados? Quais são as técnicas de anonimização que podemos utilizar?

Antes de responder estes questionamentos precisamos entender algumas verdades sobre OPSEC:

- Anonimização absoluta é praticamente uma utopia! Ou seja, por mais que utilizemos as técnicas com todo cuidado, existem técnicas de "desanonimização" que podem descobrir alguns dados sobre nossa verdadeira origem.

- A anonimização sempre tem que ser feita em camadas! Ou seja, não basta utilizar uma técnica apenas. Quanto mais técnicas utilizarmos em conjunto, mais níveis de proteção colocaremos em nossas comunicações.

- Todo cuidado é pouco! Ou seja, sempre desconfie se o seu tráfego está vazando algum tipo de dado que possa determinar a sua verdadeira origem. A paranóia poderá te salvar, não se esqueça disso.

Abaixo iremos apresentar uma série de alternativas que podem lhe auxiliar no processo de anonimização. No entanto, é sempre recomendado cautela no uso destas ferramentas pois, algumas delas, podem lhe dar uma falsa sensação de anonimização (o que reforça o fato de utilizá-las em camadas). E outras podem, infelizmente, guardar logs de acesso que poderiam ser utilizados contra você no caso de uma investigação.

A dica é sempre usar as verdades sobre OPSEC acima mencionadas para garantir o melhor nível de anonimização possível.

1. Alterando o User-Agent

Existem algumas formas de se alterar o User-Agent de um browser porém a mais simples é utilizando uma extensão chamada “User-Agent Switcher” (dentre outras), que está disponível para a maioria dos navegadores. Com ela é possível fazer o spoofing do browser e imitar as strings de user-agent de outros navegadores e sistemas operacionais, tudo isso com apenas alguns cliques.

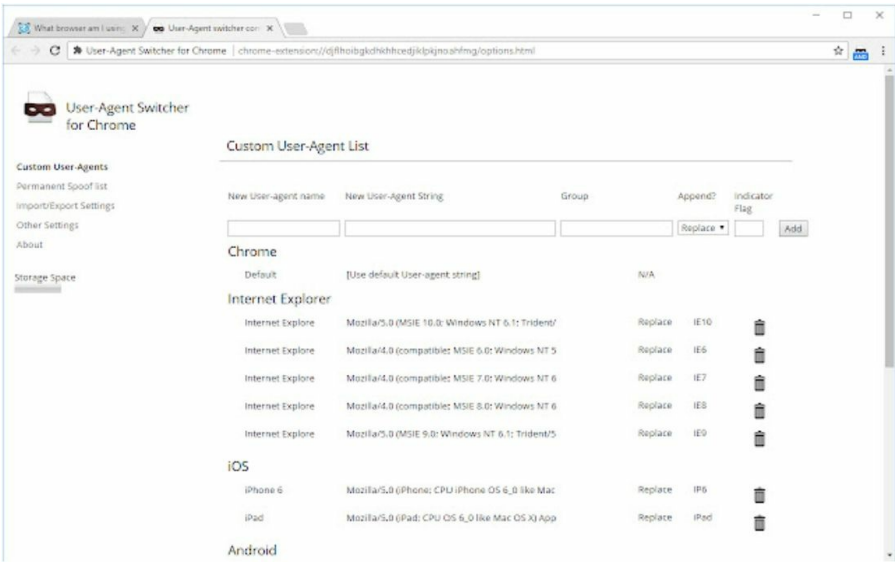


Figura 4: User-Agent Switcher no Google Chrome

2. Proxy

Servidores Proxy são uma espécie de ponte ou gateway entre você e o destino. Através deles é possível que o dado trafegado chegue no destino mascarando sua origem, uma vez que o acesso terá sido feito ao destino pelo servidor proxy e não pela sua máquina.

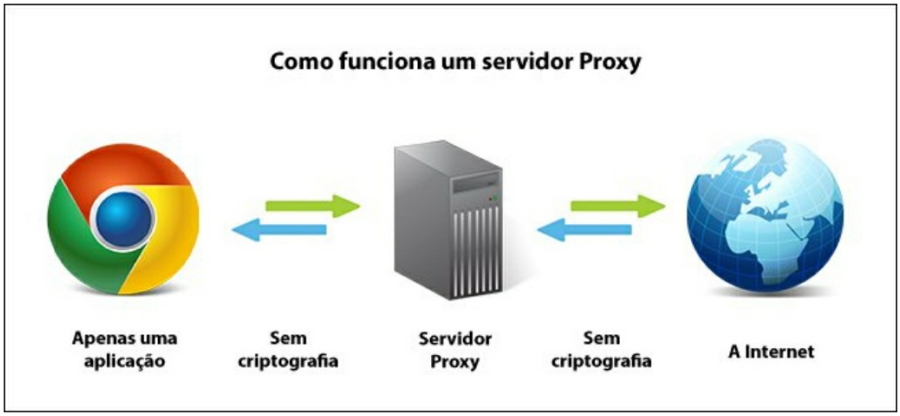


Figura 5: Funcionamento de um servidor Proxy

Para utilizar um proxy para anonimizar uma conexão basta alterar as propriedades de proxy do seu navegador com um endereço de proxy válido, que pode ser um proxy pago ou gratuito disponível na internet. Porém cabe ressaltar que uma das features de um proxy é realizar cache de acessos, ou seja, independente do serviço de proxy escolhido saiba que seus acessos são monitorados pela empresa que presta este serviço. Outro ponto ruim é que os serviços de proxy, na maioria dos casos, não provêm conexão criptografada.

Um exemplo de proxy web bem interessante é o serviço Hide My Ass, disponível em: https://www.hidemyass.com/pt-br/proxy. Com ele é possível realizar acesso a páginas através de requisições feitas pelo próprio site.

Figura 6: Serviço de Proxy Web Hide My Ass

3. VPS

O VPS (Virtual Private Server) é uma máquina virtual executada em um ambiente de Cloud, que será utilizada como servidor ponte para determinados serviços.

Há uma série de serviços de hospedagem de VPS disponíveis na Internet, onde o provedor de hospedagem cria um servidor virtual para o cliente de acordo com as especificações exigidas, por exemplo sistema operacional, capacidade de memória e armazenamento.

Nesse serviço os clientes são responsáveis por gerenciar o servidor criado, além de instalar e manter os serviços que desejam, assim como na configuração de um servidor físico. O provedor de hospedagem por sua vez mantém a estrutura física onde o VPS está instalado e garante que seja acessível aos clientes.

O VPS é um excelente aliado às ações de OPSEC, pois é possível contratar o serviço de hospedagem através de criptomoedas e acessar a máquina criada anonimamente, podendo assim manter, não só o

acesso, mas também a sua identidade. E, obviamente, é um recurso facilmente excluído em casos que se precise apagar evidências.

Existem outras tecnologias que auxiliam as ações de OPSEC do ponto de vista da anonimização, tais como VPN, TOR, I2P e etc, porém teremos capítulos dedicados a elas mais adiante, justamente por serem peças fundamentais no processo de anonimização.

Outro ponto de atenção importante é que existem alguns cuidados básicos quando se contrata qualquer serviço de terceiros com o intuito de se anonimizar. Como o próprio nome já diz são serviços de

“terceiros”, ou seja, você está estabelecendo uma relação de confiança e entregando alguns dos seus dados à eles, tais como dados de compra, dados de navegação e logs.

A dica é sempre procurar por serviços que ofereçam o maior nível de privacidade possível, que aceitem pagamentos através de moedas digitais e, principalmente, que estejam hospedados em países onde não existam leis de crimes cibernéticos (ou possuam leis brandas) e que declaram não ter parcerias com órgãos governamentais de Inteligência (CIA, NSA, FBI, ABIN e etc). E mesmo que encontre

serviços que se adequem nestas especificações, sempre pesquise sobre mudanças nas políticas de privacidade destas empresas – os órgãos de Inteligência possuem um poder muito grande para forçar empresas a se adequarem às suas regras e/ou colaborarem em casos de investigação, logo, todo cuidado é pouco.

Fingerprint

Sua “cyber digital” entrega informações sobre o seu device aos sites que você visita mesmo que os cookies e o JavaScript estejam desativados, e permite que eles distingam uma máquina cliente entre milhões de dispositivos conectados.

Você pode pensar que tais informações técnicas são genéricas e não podem ser usadas para reconhecer um determinado dispositivo, mas é ai que você se engana – pois quando essas informações são combinadas com outras informações, tais como IP, User-Agent, informações de DNS e etc, fica muito mais fácil chegar no verdadeiro autor do tráfego, mesmo que este tenha alterado algumas informações (como aprendemos antes).

Existem dois tipos principais de fingerprint: técnicas baseadas em SCRIPT e TELA.

1. Impressão digital baseada em Script

Esse tipo funciona carregando um script - geralmente um JavaScript (pode ser também através de Flash ou Silverlight) - no navegador do usuário. Este script irá executar e coletar informações técnicas sobre o navegador, bem como as especificações técnicas da máquina, tais como resolução da tela, tipo de CPU e outros detalhes sobre o Sistema Operacional. Um hash é então criado com base nas informações coletadas, que são posteriormente usadas para identificar e rastrear seu computador.

A principal defesa contra essa técnica é desabilitar o JavaScript em seu navegador. No entanto, obviamente, essa abordagem pode resultar na quebra de muitos sites.

2. Impressão digital baseada em Tela

O Canvas é um elemento HTML usado para desenhar gráficos (linhas, formas, textos e imagens) e animação em páginas web através de chamadas de APIs JavaScript. Essa técnica é explorada por diferentes atores – principalmente o mercado publicitário - para identificar dados de navegação e traçar o perfil dos usuários com o intuito de rastreá-

los.

O fingerprint de tela funciona renderizando uma imagem invisível no navegador do usuário. E uma vez carregada, a imagem coletará diferentes informações técnicas sobre o navegador e o Sistema Operacional do usuário. Novamente um hash é criado com base nas informações coletadas, isso permite que os sites rastreiem as atividades online do usuário em diferentes sites, uma vez que este hash é exclusivo para cada device.

O fingerprint é uma ferramenta poderosa para rastrear usuários, apesar de infringir em sérias questões de privacidade.

Web Real-Time Communications (WebRTC)

O

WebRTC,

conhecido

também

como

Web

Real-Time

Communications, é um projeto de software livre promovido pelo Google e Mozilla (dentre outros), que permite Comunicações em tempo real entre navegadores, usando as linguagens HTML5 e JavaScript . Tal tecnologia é pré-instalada por padrão em navegadores e Sistemas Operacionais de última geração e vem sendo amplamente usada por serviços de videoconferência como Firefox Hello, Google Hangouts, Skype (versão web), Facebook Messenger, Microsoft Teams e etc.

De acordo com uma pesquisa realizada pelo TorrentFreak, um site poderia camuflar o WebRTC em sua página com o intuito de revelar o endereço IP real de um usuário, mesmo se ele estivesse conectado a uma VPN ou a rede TOR. E se ele sabe o seu IP real, através de geolocalização, é possível identificar a localidade física do acesso.

Vamos a um teste? Se conecte a uma VPN e visite o endereço

https://browserleaks.com/webrtc. Se o seu verdadeiro endereço IP for

mostrado - não obstante a VPN ou outros sistemas falsificando seu IP

- então você está vulnerável.

Quando navegamos na web, nosso navegador deixa um canal

“aberto”, permitindo que qualquer site obtenha as seguintes informações:

• Resolução e profundidade de cor;

• Plug-ins ativos e as versões relacionadas;

• Fuso horários atuais;

• Impressão digital WebGL;

• Lista de fontes no sistema operacional;

• Idioma atual;

• Sistema Operacional e versão;

• Dispositivos externos, como um touchpad; e

• Uso de AdBlock.

Você ficará surpreso ao saber a quantidade de informações que divulgamos para os sites que visitamos. Se desejar, você pode executar um teste no site https://www.deviceinfo.me/ ou no site

https://browserleaks.com/.

Figura 7: Site www.broeserleaks.com

Protegendo a sua Privacidade

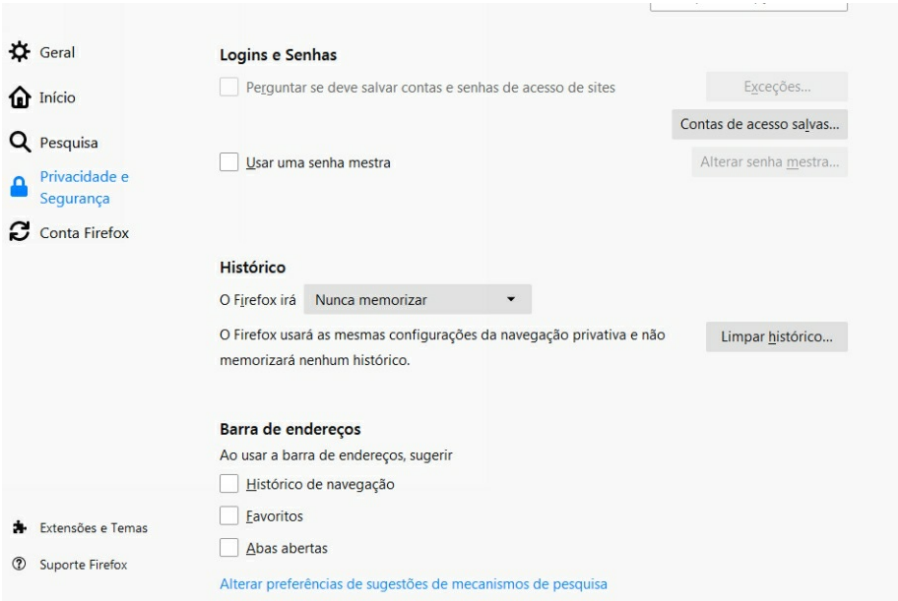
A maioria dos navegadores permite que você consiga burlar estas técnicas de rastreamento, no entanto lembre-se que qualquer técnica de anonimização NÃO DEVE ser utilizada isoladamente – sempre use várias técnicas em camada para aumentar o seu nível de anonimização.

Abaixo vamos citar uma lista (não exaustiva) de configurações que podemos realizar em nosso Firefox com o intuito de aumentar nosso nível de anonimização, e assim, garantir mais privacidade à nossa navegação:

1. Acesse as opções do Firefox clicando no menu no canto superior direito do seu navegador e selecionando **Opções**; 2. Adicione o seu mecanismo de busca padrão em:

https://addons.mozilla.org/pt-BR/firefox/addon/startpage-ssl/

(dica:



opte por um mecanismo de busca que garanta sua privacidade, como o DuckDuck Go, por exemplo).

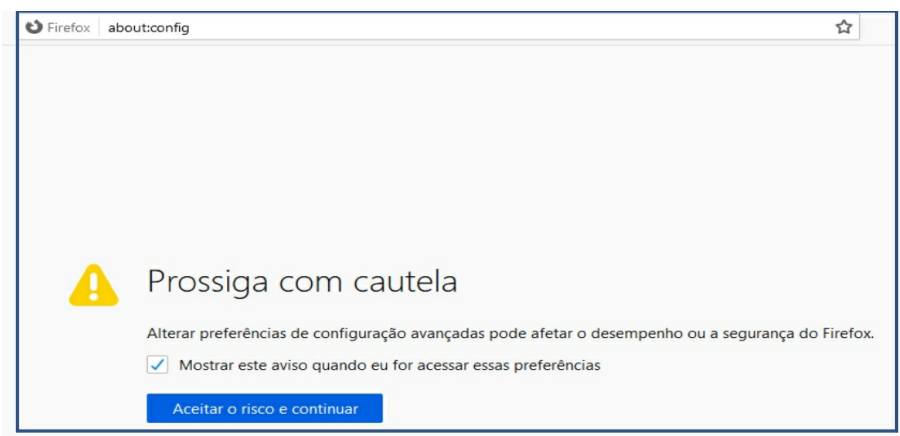
3. Vá para a guia **Privacidade e Segurança** e em Histórico configure seu Firefox para nunca memorizar.

Figura 8: Configurações de Privacidade no Firefox

5. Desativar a Coleta e Uso de Dados pelo Firefox.

Figura 9: Configurações de coleta e uso de dados no Firefox Agora que terminamos de realizar as configurações básicas do Firefox para torná-lo mais amigável à privacidade, é necessário passar para as configurações avançadas para garantirmos um nível maior de proteção.

6. Acesse a página de configurações avançadas do Firefox digitando **about:config** na barra de endereços do seu navegador.



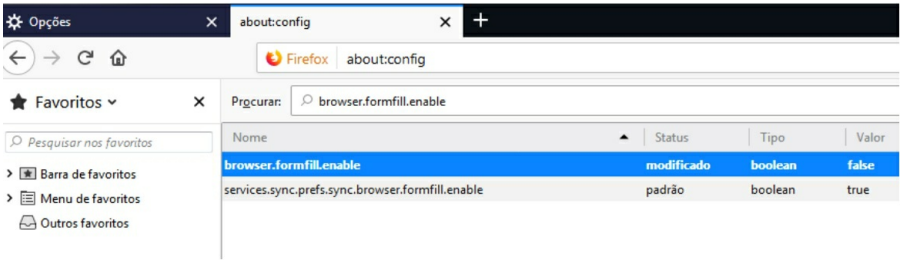


Figura 10: Configurações avançadas no Firefox

Uma mensagem de aviso aparecerá; aperte o botão "Eu aceito o risco!" para acessar o painel de configurações avançadas.

Para acessar uma configuração específica, você precisa digitar o nome dela na caixa **Pesquisar**, que aparece na parte superior da página.

Figura 11: Editando as onfigurações avançadas no Firefox 7. Para começar, vamos alterar a primeira configuração chamada **browser.formfill.enable** para **false** (clique duas vezes para alterar

o valor das configurações).

Isso força o Firefox a esquecer as informações dos formulários web. Esta opção (se habilitada) preenche suas informações automaticamente em formulários web.

8. Altere **browser.cache.disk.enable** para **false** (desta forma o Firefox não armazenará o cache em memória e no HD); 9. Altere **browser.cache.disk_cache_ssl** para **false** (desta forma o Firefox não armazenará em cache o conteúdo do disco recuperado por SSL);

10. Altere **browser.cache.offline.enable** para **false** (desta forma o Firefox não irá realizar o download de URLs para o cache offline);

11. Altere **dom.event.clipboardevents.enabled** para **false** (desta forma o Firefox não permitirá que os sites recebam notificações se o usuário copiar, colar ou cortar algo de uma página da web); 12. Altere **geo.enabled** para **false** (desta forma o Firefox não permitirá que os sites saibam sua geolocalização); 13. Altere o valor de **network.cookie.lifetimePolicy** para **2**.

Valor padrão: 0

0 = aceitar todos os cookies por padrão;

1 = aceitar apenas do site de origem (bloquear cookies de terceiros);

2 = bloquear todos os cookies por padrão;

3 = usar configurações p3p (observação: isso só se aplica a versões mais antigas do Mozilla Suite e Seamonkey.); e 4 = Política de acesso ao armazenamento: bloquear cookies de rastreadores.

14. Altere **plugin.scan.plid.all** para **false** (Irá desativar vários plug-ins nocivos, como Flash, Real Player e o plug-in do OpenOffice).

15. Altere **browser.safebrowsing.phishing.enabled** para **false** Esta configuração desativa a "Navegação segura" do Google e a proteção contra phishing. Se esta configuração for "verdadeira", o Google será capaz de verificar (e armazenar) os sites que você visita quanto à presença de malware.

16. Altere **browser.safebrowsing.malware.enabled** para **false**

Novamente, isso desativa a capacidade do Google de monitorar seu tráfego da web em busca de malware, armazenando os sites que você visita.

17. Altere **media.navigator.enabled** para **false** Os sites usam o rastreamento de mídias para ajudar a construir seu fingerprint, e uma destas táticas é rastrear o status da webcam e do microfone, por exemplo. Isso desativa a capacidade dos sites de ver e acessarem estas informações.

18. Altere **dom.battery.enabled** para **false** Outra técnica usada pelos sites para rastreá-lo é visualizar os níveis exatos da bateria. Esta configuração bloqueia essas informações.

19. Altere **extensions.pocket.enabled** para false (Desativa o serviço proprietário do Pocket)

20. Altere **default.browser.agent.enabled** para false Esta configuração refere-se apenas aos usuários de Windows. O

default-browser-agente é um deamon de sistema que é instalado

automaticamente, junto do Firefox, que tem por objetivo coletar informações sobre seu browser, mesmo quando o Firefox não está em execução.

As configurações abaixo referem-se ao WebRTC e precisam ser

alteradas para impedir que este serviço colete informações sobre o seu ambiente:

21. Altere **media.peerconnection.enabled** para false 22. Altere **media.peerconnection.turn.disable** para **true** 23. Altere **media.peerconnection.use_document_iceservers** para **false**

24. Altere **media.peerconnection.video.enabled** para **false** 25. Complementos do Firefox (extensões)

Existem milhares de extensões disponíveis para o Firefox, e algumas delas são bem úteis para aumentar nossa privacidade online:

• HTTPS Everywhere: Força o uso de HTTPS em suas comunicações,

tornando

sua

navegação

mais

segura

(https://www.eff.org/HTTPS-EVERYWHERE);

• Privacy Badge: Bloqueia anúncios de espionagem e rastreadores invisíveis (https://www.eff.org/privacybadger); e

• uBlock Origin: Bloqueador de propósito geral com regras

personalizadas definidas pelo usuário (https://addons.mozilla.org/en-

US/firefox/addon/ublock-origin/)

Conhecendo as camadas da Internet

Nem todo o conteúdo que existe na internet é indexado pelo Google e outros buscadores a que recorremos quando queremos pesquisar uma informação. Logo, temos uma “Internet paralela” onde tudo que você faz ou acessa é oculto aos usuários normais, e que para acessá-la, precisaremos de softwares específicos.

Um estudo da Cuponation revelou que em 2021 haviam cerca de 4,66 bilhões de usuários ativos na Internet, o que representa aproximadamente 59,5% da população mundial. Porém estes dados

referem-se somente a uma parte da Internet… a Surface.

Essa é a parte da Internet que inclui todo o conteúdo que está disponível ao público. Os sites da Surface podem ser indexados usando mecanismos de pesquisa regulares, como o Google, para que um usuário possa encontrá-los facilmente.

Estes buscadores utilizam, dentre outras tecnologias, alguns bots para descobrir novas páginas a todo momento. Estes bots trabalham

“clicando” em links nos sites e enviando essas páginas (resultados) para os servidores dos mecanismos de pesquisa, os quais organizam os resultados em um índice de pesquisa.

Não irei me ater muito na surface pois não é o nosso objetivo (e tenho certeza que, mesmo de forma empírica, você já sabe muito bem o que é essa camada, não é mesmo?)

Deep Web

Pode se dizer que a Deep Web é responsável pela maioria das lendas urbanas atuais. Muitos usuários replicam fábulas e casos que ouviram (ou leram) na Surface (superfície da Internet), sem se quer nunca ter tentado entrar na Deep. O desconhecimento é tanto que

até alguns “especialistas” usam os termos Deep Web e DARK Net como sinônimos, apesar de haver uma grande diferença entre eles.

O termo Deep Web descreve todos os recursos on-line que não são indexados usando mecanismos de pesquisa convencionais, como Google, Bing ou Yahoo, mas a Deep Web ainda pode ser acessada como qualquer site comum usando o protocolo padrão da web HTTP/ HTTPS, bem como os navegadores comuns, sem usar nenhum software especial. Qualquer usuário da Internet certamente usou algum tipo de Deep Web enquanto navega na Internet; no entanto, a maioria dos usuários pode não saber que esses recursos pertencem à Deep Web.

Os recursos da Deep Web geralmente não são indexados nos mecanismos de busca, fazendo com que um usuário que deseje acessar estes recursos precise saber o endereço correto do seu destino. Ou ainda são recursos que, para serem acessíveis, necessitam de algum tipo de camada de segurança, tais como credenciais de acesso e/ou VPN.

Em outras palavras, se a intranet da sua empresa não está indexada no Google (pelo menos não deveria!), ela faz parte da Deep Web.

Ninguém pode conhecer o volume exato de sites da Deep Web devido à natureza de constante mudança e falta de indexação (obviamente), mas muitos estudos sugerem que é aproximadamente 500 vezes o da Surface. Aqui estão alguns exemplos de sites que compõem a Deep Web:

SITE

DESCRIÇÃO

A maior biblioteca online do mundo, que

inclui uma enorme coleção de recursos - como https://www.loc.gov

livros, fotografias, arquivos de jornais, mapas e etc.

Fornece acesso a certidões de nascimento, https://www.vitalrec.com

registros de óbito e licenças de casamento nos EUA.

Dá acesso a mais de 200 milhões de páginas

https://www.science.gov

de informações científicas oficiais.

Fornece acesso aos Jornais/periódicos de alta

https://doaj.org

qualidade, acesso aberto e com revisão por pares.

Dá acesso gratuito a mais de dois milhões de

http://onlinebooks.library.upenn.edu livros acessíveis (e legíveis) na Internet.

https://www.100searchengines.com

Buscador focado em privacidade

Dark Net

Agora, chegamos à terceira camada da Web. Dark Net - ou Dark Web - é um ambiente na Internet que foi projetado propositalmente para ser oculto e anônimo. A Dark Net forma uma pequena parte da Deep Web, mas, diferentemente da Deep Web, esta não pode ser acessada usando

navegadores comuns.

As redes Dark Net - ou Redes de Anonimato - são compostas de coleções de computadores espalhados por todo o mundo que formam uma rede descentralizada. Os usuários podem acessar essas redes para navegar anonimamente na Web ou para visitar sites ocultos anônimos nessas redes.

Os indivíduos chegam à Dark Net para vários propósitos, e um número significativo deles são ilegais. Embora não haja estatísticas precisas sobre a quantidade de sites ilícitos, o grupo Intelliagg analisou em 2015 mais de 1.000 amostras de serviços ocultos na Rede Tor e constatou que 68% do conteúdo da Dark Net é ilegal. Os

criminosos não estão apenas visitando a Dark Net para procurar produtos ilegais, mas estão utilizando-o como um meio para anonimizar suas correspondências on-line e impedir que outros os rastreiem. Ainda assim, embora a maioria dos sites da Dark Net esteja associada a atividades ilegais, muitas pessoas o utilizam para fins legítimos.

Existem diferentes Redes de Anonimato. As seguintes são os mais populares:

- Tor: https://www.torproject.org

- I2P: https://geti2p.net

- Freenet: https://freenetproject.org

Quem acessa a Dark Net?

A Dark Net tem uma má reputação por ser o local preferido para atores mal-intencionados realizarem suas atividades criminosas online.

A seguir estão alguns exemplos:

I. Os traficantes de drogas que exploram o recurso de anonimato da Dark Net para realizar suas vendas ilegais com segurança; II. Os traficantes de armas usam a Dark Net para compra e venda ilegal de armas.

III. Compradores de documentos falsos do governo (como Passaportes, por exemplo);

IV. Cibercriminosos o usam para negociar exploits; vender ataques de

negação de serviço distribuído (DDoS), ransomware, malwares e etc.;

V. Terroristas usam a Dark Net para compartilhar informações e negociar ilegalmente, além de ocultar suas atividades na Web de superfície.

VI. Jogadores de sites de apostas; e VII. Os vendedores de informações roubadas - como segredos corporativos, números de cartão de crédito e informações pessoais obtidas durante atividades fraudulentas.

Embora muitos sites da Dark Net sejam direcionados a atividades criminosas, há aqueles que a utilizam para fins legais, tais como: I. Ativistas de direitos humanos, jornalistas e denunciantes o usam para revelar conteúdos secretos ao público, sem revelar sua identidade;

II. Os defensores da privacidade usam a Dark Net anonimamente, longe dos governos e da vigilância corporativa;

III. As organizações de segurança pública usam a Dark Net para diferentes propósitos (por exemplo, rastrear criminosos e coletar informações sobre eles).

IV. Indivíduos, governos e corporações usam redes de anonimato como um meio seguro para trocar informações ultra-secretas; V. Os serviços de inteligência e organizações militares usam a Dark Net para coletar informações de inteligência de código aberto e combater atividades terroristas;

VI. As empresas podem monitorar fóruns e blogs da Dark Net para ver suas próprias informações proprietárias vazadas; E talvez você se pergunte como os usuários fazem seus negócios anonimamente na Dark Net. A resposta é simples. Todo site na Dark Net aceita pagamento por bitcoins e outras criptomoedas.

Nos próximos capítulos iremos apresentar cada uma destas Redes de Anonimato.

Rede Tor

O Projeto Tor foi originalmente desenvolvido pelo Laboratório de Pesquisa Naval dos Estados Unidos, junto com o matemático Paul Syverson e os especialistas em computação Michael Reed e David Goldschlag na década de 1990, tendo como objetivo proteger as comunicações militares de Inteligência através de camadas de criptografia, as quais deveriam aumentar o anonimato dos usuários online.

Anos mais tarde o Laboratório de Pesquisa Naval liberou o código-fonte do projeto sob uma licença gratuita, o que fez a Electronic Frontier Foundation (EFF) se juntar como financiadora e apoiadora do projeto, embora ainda se passassem mais alguns anos antes que a organização sem fins lucrativos por trás da fundação Tor fosse fundada.

O que exatamente é o Tor? Em sua forma mais básica (pois existem outras formas de implementação), o projeto Tor é composto de duas partes: um navegador que permite que os usuários se conectem à rede Tor e um sistema global de retransmissões, projetado para entregar de forma anônima o conteúdo solicitado. O

uso do Tor fornece uma maneira mais segura de se navegar na Internet sem entregar o verdadeiro IP do dispositivo ou qualquer uma das informações visualizadas durante a sessão.

Porém precisamos deixar claro um fato importante: como veremos mais a diante, a rede Tor é provida através de servidores voluntários.

Ou seja, qualquer um pode subir um servidor na rede e servir como nó de acesso (relay). O impacto disso é que, sendo um nó de acesso, este servidor saberá o hop anterior da requisição, bem como o próximo.

Muitas agências de Inteligência tem mantido servidores na rede

Tor com o intuito de correlacionar o tráfego que passa por eles e, desta forma, conseguir chegar na verdadeira origem do tráfego. Claro que estas ações visam a captura de criminosos que usam a rede para fins ilícitos, porém nos serve de alerta para entendermos que não existe anonimato absoluto na rede Tor. E como já mencionei anteriormente, todo processo de anonimização precisa ser feito em camadas ao contrário de depender somente de uma tecnologia e/ou serviço.

Como o Tor funciona tecnicamente?

Quando um usuário deseja conectar-se a um sistema remoto através da rede TOR, esta estabelece o enlace através de um circuito de Onion Routers. Para acessar a rede TOR, o usuário precisa executar, localmente, um programa chamado Onion Proxy e este cuidará da conexão entre o usuário e a rede TOR. Cada usuário executa localmente um software chamado onion proxy para buscar diretórios, estabelecer circuitos através da rede, e manipular as conexões das aplicações do usuário.

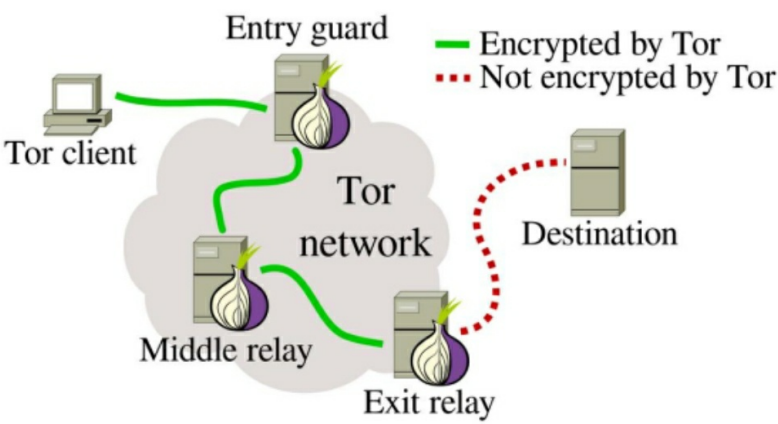
A rede TOR foi desenhada para funcionar sobre o protocolo TCP.

Para isso, utiliza o protocolo SOCKS, versão 5, o qual foi definido na RFC 1928, de março de 1996. Esse protocolo permite que exista um intermediário entre os elementos de uma conexão TCP ou UDP. Como observamos na figura abaixo, as solicitações de conexão de um usuário são enviadas para um servidor que utiliza o protocolo SOCKS

e este reencaminha-as para o endereço com o qual ele deseja conectar-se. A resposta é enviada para o serviço SOCKS que a encaminha para o usuário. Por essa capacidade, o protocolo SOCKS

tornou-se a base dos servidores proxy que são amplamente empregados em redes corporativas. A rede TOR utiliza este protocolo pois é suportado pela maioria das aplicações baseadas em TCP e torna desnecessário a criação de soluções próprias.

A rede estabelece um circuito formado por três Onion Routers (ou



relays), antes de estabelecer a conexão entre o usuário e o destinatário com o qual este deseja se conectar. Observemos a seguinte imagem:

Figura 12: Topologia da Rede Tor

Logo, temos três elementos:

1. Guards: são os Onion Routers com os quais o Onion Proxy, ativado pelo usuário, conecta-se. São responsáveis por conectar o cliente à rede TOR, bem como retransmitir os dados para os demais

‘nós’ da rede. Devido a criptografia realizada no cliente, o Guard desconhece o endereço do destino final dos dados, restando somente a informação do endereço do próximo nó.

2. Middle-Relays: são ‘nós’ intermediários responsáveis por encaminhar o fluxo de dados ao próximo Relay ou até um Exit-Relay.

3. Exit-Relay: é o Onion Router que se conecta ao endereço

solicitado pelo usuário e que descriptografa os dados criptografados pela rede TOR. São ‘nós’ responsáveis pela comunicação com o destino final.

Para manter seus usuários anônimos, a rede TOR estabelece diversos padrões. Ela busca impedir que a identidade do usuário seja identificada através do mascaramento do seu endereço IP, mas também evita que sua localização seja definida e que uma possível análise de tráfego seja realizada, impedindo que um perfil seja traçado.

Por trafegarem por vários Onion Routers, os administradores dos sistemas que funcionam como Onion Router poderiam acessar os dados dos usuários, caso trafegassem sem nenhuma criptografia. Se os dados fossem criptografados com uma chave comum a todos os elementos do circuito estabelecido, caso um Onion Router fosse comprometido,

ele

poderia

forçar

outro

Onion

Router

a

descriptografar os dados e, então, acessar as informações. Para evitar essas duas situações, o Onion Proxy sendo executado no sistema computacional do usuário estabelece uma chave simétrica com cada um dos Onion Router que participem do circuito estabelecido. O Onion Proxy criptografa os dados do usuário com todas as chaves criadas, como se fossem camadas, e cada um dos Onion Router retira uma camada da criptografia utilizando sua respectiva chave. Dessa forma, mesmo que um Onion Router esteja observando os dados de um usuário durante a transmissão de dados, ele terá acesso apenas ao endereço do próximo salto e do local de onde os dados estão vindo, mas não da origem.

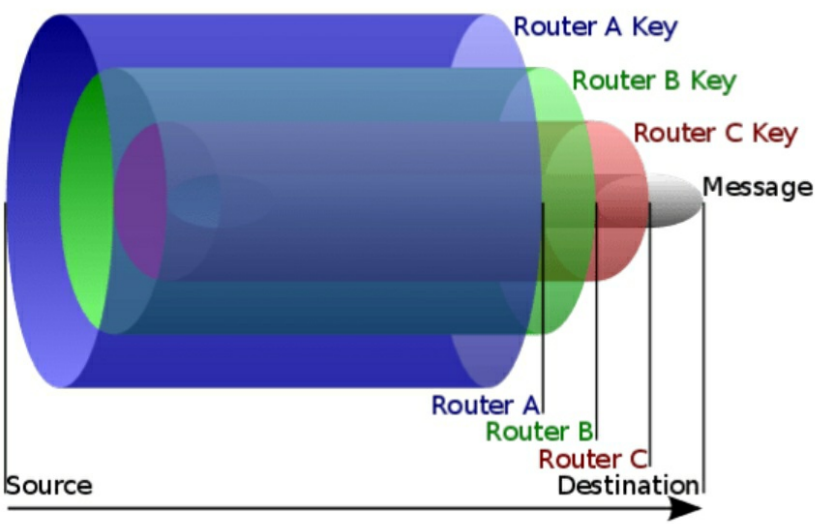


Figura 13: Camadas criptográficas da Rede Tor

Como podemos observar na imagem acima, as mensagens que trafegam entre o nó de saída (Exit Relay) e o servidor não serão

criptografadas e poderão ser analisadas caso esse nó seja comprometido. Dessa forma, pode-se inserir mais um nível de segurança utilizando uma conexão segura como o HTTPS ou TLS.

Um circuito pode ser utilizado para transmitir vários streams de pacotes TCP. A Rede TOR multiplexa múltiplas conexões TCP através de um circuito para aumentar a eficiência e anonimidade. Esse comportamento dificulta a identificação de uma única conexão e sua análise, o que poderia identificar o usuário da rede TOR através de uma análise comportamental.

Para identificar os OR e seus estados atuais, a rede TOR utiliza servidores de diretório (Directory Servers), os quais são um pequeno número de OR bem conhecidos. Esses servidores disponibilizam a lista

dos OR via HTTP e o usuário a utilizará para acessar a rede TOR e montar os circuitos de roteadores. Isso evita que algum atacante manipule a criação dos circuitos e direcione os dados de um usuário para um local específico.

Como usar a Rede Tor?

Para facilitar o acesso à rede TOR, o projeto TOR começou a desenvolver vários projetos para muitas variações de navegação, incluindo:

1. Tor Browser, contendo:

a) Pacote com navegador (Firefox);

b) O plugin HTTPS Everywhere (forçando conexões SSL); c) O plugin NoScript (bloqueando o JavaScript); e

d) Torclient.

Ele está disponível em versões instaláveis e portáteis para todos os sistemas.

https://www.torproject.org/download/

2. Orbot

Ele é um cliente que permite a conexão com a rede TOR e protege o tráfego de dados de todos os aplicativos em dispositivos Android.

https://guardianproject.info/apps/org.torproject.android/

3. Tails

Ele é uma distribuição GNU/Linux, que foi desenvolvida para navegação anônima e permite transmitir a conexão à rede TOR. Ele também oferece ferramentas para criptografia e anonimato.

https://tails.boum.org/

4. Atagar

Ferramenta de linha de comando utilizável para controlar e configurar a rede TOR.

https://www.atagar.com/

5. Atlas

Uma ferramenta online com a qual você pode verificar o status dos relés online TOR.

https://atlas.torproject.org

6. Pluggable Transports

Aqui você encontrará programas de fornecedores terceirizados com suporte para anonimato.

https://2019.www.torproject.org/docs/pluggable-

transports.html.en

7. OONI

Software usado por governos para detectar abuso de tráfego e monitorar nossa conexão.

https://ooni.org/

Instalação do Tor no GNU/Linux (Debian / Kali)

Apesar de estar disponível para Windows, Mac OS e GNU/Linux, iremos cobrir a instalação em ambientes GNU/Linux (Debian-like, como o Kali Linux). Para conferir os detalhes da instalação em outros

Sistemas Operacionais, acesse: www.torproject.org/

Primeiro vamos atualizar nosso repositório local:

apt-get update

E seguir com a instalação dos pacotes do Tor em nosso ambiente:

apt install apt-transport-https tor deb.torproject.org-keyring torsocks torify torbrowser-launcher -y

Com as configurações acima podemos utilizar o Tor via Terminal, com o SSH por exemplo, bem como tornar a nossa máquina um relay da Rede. E pra isso, iremos realizar uma série de configurações.

Usando o seu editor de textos preferido, edite os arquivos abaixo (usaremos como exemplo o vim):

vim /etc/tor/torrc

No fim do arquivo, adicione as seguintes linhas:

HiddenServiceDir /var/lib/tor/other_hidden_service/

HiddenServicePort 22

Salve e saia do arquivo. Agora você deve restartar o serviço do Tor com o comando abaixo:

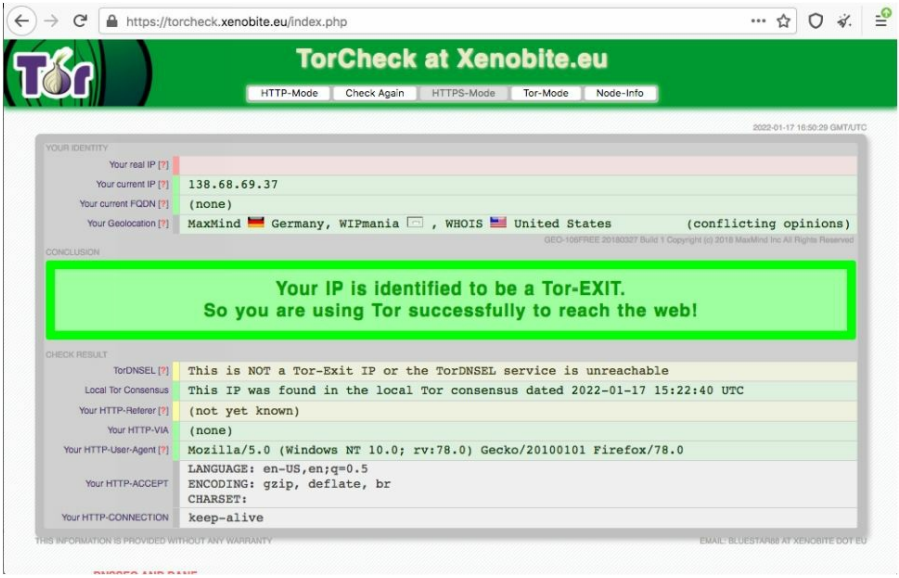
systemctl restart tor

Ao reiniciar o serviço, o Tor irá gerar os arquivos necessários em

/var/lib/tor/other_hidden_service. Inclusive neste diretório você encontrará o hostname da sua máquina na rede Tor.

O hostname fica no seguinte arquivo:

#cat /var/lib/tor/other_hidden_service/hostname



Você verá algo como **xyzabcdefyte.onion**

Para proteger suas conexões SSH você pode usar o torify, desta forma:

torify ssh user@hostname

Como durante a instalação também baixamos o lançador do Tor Browser, basta abri-lo via menu de aplicativos para acessá-lo. E

através do site TorCheck, mantido pela Xenobite, é possível verificar se você está usando o Tor Browser com todas as configurações corretas. https://torcheck.xenobite.eu/index.php.

Figura 14: Conferindo o acesso via Tor Browser

Rede Privada Virtual (VPN)

As VPNs foram originalmente projetadas para criar uma “LAN de computadores conectados pela Internet”, como uma rede física porém sem todos os custos envolvidos, bem como fornecer uma solução para o envio de tráfego sensível através de redes inseguras.

Uma ligação VPN geralmente é referida como um túnel, e é uma ligação encriptada entre dois pontos. Esta é geralmente criada através da utilização de um cliente de VPN de um lado da ligação e um Servidor VPN (ou gateway) na outra extremidade. O cliente utiliza uma aplicação para se autenticar no Servidor VPN, geralmente através

da internet, e depois da ligação estar estabilizada, todo o tráfego é alterado da interface normal de rede para o túnel encriptado da VPN.

As VPNs são também utilizadas para proteger ou anonimizar um tráfego através de uma conexão não segura (como a internet, por exemplo). Há empresas que provêm este tipo de serviço com o intuito de impedir que os conteúdos do tráfego dos seus clientes sejam armazenados nos ISPs ou de serem capturados por outros usuários, permitindo também esconder a localização geográfica do utilizador, entre outros aspectos.

Estes serviços são também populares em relação aos sistemas que envolvem compartilhamento de dados peer-to-peer (P2P). Tal atividade é geralmente limitada pelos ISPs por questões de violação de direitos autorais. Neste contexto, as VPNs podem permitir o tráfego e esconder os verdadeiros endereços de IP neste tipo de conexão.

Quanto ao tipo (e não ao protocolo) podemos encontrar pelo menos três classificações de VPN no mercado: VPN confiável, VPN

segura e VPN híbrida.

Neste capítulo, abordaremos VPNs seguras, porque VPNs confiáveis requerem acordos especiais com ISPs e não são facilmente aplicáveis a casos comuns; elas são projetadas quase que exclusivamente para redes corporativas, onde a entrega de informações aos destinatários deve ser sempre garantida.

As VPNs híbridas, por outro lado, são a combinação de confiável e segura e, como não vamos cobrir o primeiro, também excluiremos o último.

A qualidade de uma VPN em termos de segurança é determinada pelos tipos de protocolo e pela segurança das chaves fornecidas -

além das políticas e estabilidade do serviço, como veremos adiante.

Protocolo PPTP

O PPTP (abreviação de Point-to-Point Tunneling Protocol) foi desenvolvido pela Microsoft para criar empresas VPN por discagem telefônica. Isso foi projetado exclusivamente para VPNs e geralmente depende do MS-CHAP para gerenciar a autenticação.

Devido à popularidade conquistada ao longo dos anos, essa ferramenta pode ser facilmente instalada (ou pré-instalada) em qualquer

dispositivo do mercado. Além disso, é rápida e requer recursos limitados. O protocolo PPTP suporta apenas 128 bits de chave criptográfica e perdeu terreno devido a vulnerabilidades encontradas, até que a Microsoft o declarou inseguro em 2012, apesar das dezenas de patches lançados para garantir a eficiência.

O protocolo é considerado inseguro e provavelmente já foi violado pela NSA. No entanto, o PPTP ainda é útil para atividades com latências baixas, como jogos na Internet, Torrent, streaming e assim por diante.

L2TP/IPSec

O L2TP (abreviação de Layer 2 Tunnel Protocol) é um protocolo VPN que sozinho não garante a proteção de dados. É por isso que muitas vezes é integrado ao pacote IPSec. Ele combina o protocolo de encapsulamento com criptografia e já vem implementando Sistemas Operacionais mais novos. Isso permite uma configuração fácil pelo cliente, bem como uma boa velocidade em geral.

Até então nenhuma vulnerabilidade crítica foi identificada para este protocolo, logo ele é recomendado se você quiser manter uma boa privacidade e segurança. No entanto, pesquisas feitas por alguns especialistas do setor sugerem que a NSA está constantemente tentando quebrá-lo, embora isso ainda não tenha sido comprovado (ou divulgado).

O L2TP/IPsec oferece encapsulamento de dados de dois níveis com chaves de criptografia de 256 bits. Embora mais lento que o PPTP, o suporte multi-threaded implementado em kernels mais recentes permite que a arquitetura de processadores multicore seja usada para criptografar e descriptografar operações. A única pequena desvantagem é que o L2TP usa a porta UDP 500 padrão, que geralmente é bloqueada por firewalls corporativos e requer encaminhamento de porta em roteadores.

OpenVPN

O OpenVPN é um software de código aberto, especialmente desenvolvido para criar túneis criptografados (SSLv3/TLSv1) entre dois sistemas. Ele é totalmente aberto e transparente o suficiente para ser considerado a solução mais confiável e segura.

Atualmente, o risco de ser vazado por uma agência de Inteligência do governo é mínimo. Justamente por ser um código aberto, você pode configurá-lo de acordo com sua preferência e usá-lo em qualquer

porta, sem encaminhamento de porta (ou seja, também usar TCP 443 para processar solicitações HTTP sobre SSL).

A biblioteca de criptografia usada (OpenSSL) pode ter várias cifras (como Blowfish, AES, DES etc.). No entanto, a maioria das VPNs usa cifras AES ou Blowfish quase que exclusivamente. O último é baseado em 128 bits e é a criptografia padrão no OpenVPN.

Este protocolo é mais lento que o IPSec e pode ter um impacto negativo em dispositivos com capacidade de processamento limitada, pois não há suporte nativo para multithreading. Portanto, não é possível usar CPUs de última geração. Embora a dissonância seja um padrão de fato como o PPTP e o L2TP/IPsec mencionados, o OpenVPN foi bem-vindo no mercado de provedores de VPN, tendo atualmente capilaridade em quase todos os dispositivos, incluindo mobile.

Como escolher uma VPN para uso em OPSEC?

Se fossemos listar aqui as principais VPNs e fazer um comparativo entre elas, seria improdutivo devido as constantes mudanças do mercado, cenários políticos e etc. No entanto, decidi separar algumas dicas que são fundamentais na hora de escolher uma VPN, principalmente para ações de OPSEC:

a) **Evite VPNs gratuitas**. Já comentamos anteriormente que, se você não paga por algo, você é o produto. Logo, utilizar uma VPN

grátis, ainda mais para fins de atividades de OPSEC, seria no mínimo falta de profissionalismo. E claro que, ao invés de algo free, sempre buscamos otimizar nossos gastos (principalmente quando estamos em um país com uma taxa de câmbio bem alta frente ao dollar). Para isso sempre tenha em mente:

Regra nº 1: há um custo associado à manutenção dos serviços VPN. Alguns dos melhores serviços VPN oferecem mais de 1000 servidores em todo o mundo, e é fato que existem custos para mantê-los, custos para substituir dispositivos defeituosos e custos para gerenciá-los. Por tanto, sabendo que não existe almoço grátis, você nunca deve confiar em VPNs grátis!

Regra no 2: os provedores podem vender seus dados.

Como você acha que se monetiza uma VPN? Simplificando, os provedores podem vender seus dados. Não estou falando somente de nomes de usuário e senhas. Até o que se acessa, quando se acessa e etc podem ser utilizados, dentre outras coisas, são informações

consumidas por empresas de benchmark e pelo mercado de marketing.

Regra no 3: os provedores podem reutilizar nossa largura de banda. Assim que estiver online, você fará parte da rede virtual e, portanto será mais um asset. Sua conexão com a Internet ficará lenta (obviamente) e você poderá ser o "fim da linha" e ser responsável pelas práticas ilegais de outros usuários.

Regra no 4: os fornecedores podem bombardeá-lo com publicidade. Esta é uma prática comum para proxies e VPNs gratuitos.

Adware em VPNs gratuitos pode ser incorporado ao cliente ou exibido enquanto você está navegando, alterando o HTML das páginas da web que esteja acessando.

Regra no 5: você não está protegido. Ao comprar um serviço, você está protegido por um documento com o qual você e a empresa concordam automaticamente com os 'Termos de uso'. Juntamente com a política de privacidade, é o documento legal que regula a relação entre as partes. Quando se trata de VPNs gratuitas, por mais confusos que sejam os documentos, os usuários tendem a pensar:

"Contanto que seja gratuito, quem se importa?" Como iremos descobrir em breve, os termos de serviço e as diretrizes de proteção de dados garantem a qualidade da VPN, bem como a eficiência e segurança na navegação.

b) A política de Logs

Os Logs são arquivos gerados para cada atividade realizada em um sistema de TI: no caso das VPNs, os logs podem salvar IPs e

outras informações não criptografadas. Ou seja, seus dados estão nas mãos de terceiros, e o pior, você pode não ter controle sobre nada disso.

Imagine que você é o dono de uma empresa VPN e o FBI (ou a CIA, a polícia ou qualquer outra pessoa) chama bate a sua porta com um mandado para pesquisar dados em seus servidores. Você gostaria de ser um guerreiro da justiça e proteger alguém que você não conhece, que possivelmente brincou com o mainframe de alguma corporação no outro canto do planeta? É desnecessário dizer que a resposta é não. Não há provedores de VPN que arriscariam anos de prisão por você. (lembra que comentamos antes que uma das dicas para saber quais serviços contratar na hora de anonimizar? Saber se a empresa da sua

VPN tem sede em um país com leis severas do ponto de vista cibernético, ou é aliado de grandes potências mundiais, é extremamente importante).

Portanto, lembre-se de que um provedor de VPN não poderá divulgar informações sobre você se ele não as tiver; portanto, você não pode ser processado por não possuir dados que não estejam realmente em sua posse. Sempre use mais de uma camada de proteção para sua conexão e, em último caso, nunca forneça seus dados reais no momento de uma contratação.

c) Leis internacionais de retenção de dados

Apenas um exemplo do mundo real: a NordVPN é uma empresa localizada no Panamá, um país que quase não tem restrições em termos de leis de retenção de dados. Sem surpresa, também é definido como um paraíso fiscal, onde 120 bancos atendem secretamente a empresários ricos (incluindo sonegadores de impostos) e empresas offshore. Lá, as empresas não são obrigadas a apresentar demonstrações financeiras e os residentes podem decidir não apresentar suas declarações de imposto de renda, então por que os revendedores VPN locais armazenariam dados fiscais de clientes?

Não estou afirmando que é a melhor do ponto de vista da privacidade,

no entanto, se tiver que escolher entre uma VPN sediada nos EUA ou a Nord, certeza que escolheria a Nord.

d) Métodos de pagamento

As características que distinguem uma VPN segura de uma não segura incluem os métodos de pagamento suportados. Se você está pensando em alugar uma VPN com serviços de pagamento como PayPal, cartão de crédito ou transferência bancária (usando seu nome), lembre-se de que deixará dados importantes nas mãos deles.

Não importa o quão forte seja a política de privacidade de VPN, os bancos armazenarão seus detalhes de pagamento (não só os bancos, mas os governos também).

Uma VPN que aceita apenas pagamentos rastreáveis (cartão de crédito, transferência bancária, ordem de pagamento, etc.) não pode ser definida como uma VPN segura.

Nesse caso, você deve preferir uma VPN que ofereça pagamentos em criptomoedas, como Bitcoin por exemplo, e tome as devidas

precauções para evitar a exposição de suas carteiras a riscos de rastreabilidade.

e) Lista de VPN interessantes

Este site correlaciona a lista atualizada das melhores VPNs disponíveis no mercado, citando informações importantes tais como suas políticas de privacidade, se elas não armazenam seu IP, protocolos suportados, política de logs, país, questões de privacidade e formas de pagamento.

https://www.safetydetectives.com/best-vpns/

Avaliando a segurança da sua VPN

Após a escolha da sua VPN, chegou a hora de avaliar o nível de segurança e privacidade de sua VPN. Nós faremos alguns testes

simples para que possamos garantir que nossos dados estão protegidos.

Além dos testes realizados no capítulo sobre as técnicas de anonimização, os quais podem ser amplamente utilizados aqui também, podemos utilizar o serviço IPLeak para avaliar as informações que podem estar sendo vazadas da nossa conexão.

Figura 15: Conferindo se há vazamentos em nossa VPN

Outro ponto super importante de ser analisado é se há vazamentos de DNS em nossa conexão. Imagine que você está utilizando uma VPN muito boa, usando a rede Tor como mais uma camada de proteção bem como alguns plugins e configurações de privacidade em seu

navegador, porém não se atentou ao seu DNS… o que isso poderia lhe trazer de problemas? Muita coisa! Ao chegar no destino uma requisição de um IP oriundo do Paquistão, por exemplo, utilizando o DNS do Brasil, seria tão incomum que faria qualquer Analista de Segurança monitorar seu tráfego e/ou comportamento –

dessa forma você estaria agindo na contramão do Low Profile as a Lifestyle.

Existem vários serviços online para testar e verificar se há

"vazamentos" em sua conexão, como o www.dnsleaktest.com/ por exemplo. Nunca deixe de avaliar constantemente se sua conexão está vazando informações de DNS, pois casos simples como este podem colocar toda uma ação de OPSEC em risco.

Freenet

A Freenet é um projeto do irlandês Ian Clarke e foi criada exatamente para oferecer um ambiente seguro, privado e eficiente para os seus usuários. O projeto foi iniciado em Março de 2000, em uma versão que continha pouco em comum com a Freenet atual, porém que já visava solucionar problemas centrais para a criação de uma rede anônima eficiente.

O projeto foi criado na plataforma Java e queria oferecer não somente um lugar para os usuários poderem se comunicar de forma aberta, mas também compartilhar arquivos e utilizar ferramentas privadas de microblogging. Para isso, Ian Clarke tomou uso de técnicas fundamentais de computação, como o uso de sistemas de dados distribuídos e de diversos modos de criptografia.

Um dos fatos que comprovam a significância do sistema Freenet para a concepção do anonimato na internet é do artigo de Clarke que inicialmente concebeu a idéia da Freenet. "Freenet: A Distributed Anonymous Information Storage and Retrieval System" foi o artigo mais citado na área de ciência da computação do ano de 2000. Além disso, o sistema já foi centro de diversos artigos no New York Times, BBC e CNN.

Funcionamento da rede Freenet

A Freenet sofreu uma mudança drástica em 2008, com o lançamento da versão 0.7. Até então, a Freenet operava em um modo que oferecia uma forte segurança para os seus usuários, mas que ainda não utilizava todo o potencial tecnológico para prover uma privacidade

completa. Este modo é atualmente chamado de Opennet, e, o criado para melhorar as questões de privacidade e segurança é chamado de Darknet. Atualmente a Freenet permite que o usuário trafregue na rede utilizando qualquer um dos dois modos.

O sistema é feito a partir da criação de uma rede onde os usuários estabelecem conexões entre si para transmitir informações pela rede.

Um usuário não tem conexão com a rede inteira, mas sim apenas com alguns outros usuários, e através de mecanismos de roteamento ele consegue transmitir e buscar dados na rede inteira.

Cada usuário (também chamado de nó) recebe um identificador especial ao ser inserido na rede, que é um valor circular entre 0 e 1

(portanto 0 e 1 correspondem ao mesmo identificador). O mapa da rede é então dado através de um círculo onde os usuários são alocados em seu perímetro. Dessa forma, a distância máxima entre dois usuários é de 0.5.

A página oficial do projeto é freenetproject.org

Instalação em GNU/Linux

Apesar de estar disponível para Windows, Mac OS e Linux, iremos cobrir a instalação em ambientes GNU/Linux (Debian-like, como o Kali Linux). Para mais informações sobre a instalação em outros Sistemas Operacionais, acesse: https://freenetproject.org/pages/download.html

Usando o seu terminal, execute o comando abaixo para efetuar o download do arquivo instalador:

#

wget

'https://github.com/freenet/fred/releases/download/build01492/new_installer_offline_1492.jar'

-O new_installer_offline.jar

Agora basta rodar o instalador com o java, assim:

java -jar new_installer_offline.jar

Figura 16: Executando o instalador do Freenet

Quando o instalador fechar, ele deverá abrir uma janela do navegador apontando para o Wizard de configuração do Freenet. Nele você pode definir as configurações básicas e, em seguida, começar a usar o Freenet.

Você pode acessar o Freenet mais tarde através do ícone gerado no menu de aplicativos do seu sistema, porém caso ele não funcione, abra http://127.0.0.1:8888/ em seu navegador.

Na minha Wiki eu cito uma lista (atualizada) de sites e repositórios interessantes

na

Freenet,

em:

https://sejalivre.org/vinicius/index.php/Freenet#Links

Invisible Internet Project (I2P)

O projeto I2P (Invisible Internet Project) nasceu no ano de 2003

através de um grupo de desenvolvedores e pesquisadores de segurança, com objetivo inicial de criar uma rede virtual privada que fosse resistente a censura e tivesse um bom nível de desempenho e estabilidade. Suas bases funcionais são similares a outras como o TOR, porém existem importantes diferenças que fazem do I2P em uma alternativa bastante potente em termos de privacidade e anonimato.

O I2P permite a criação de qualquer tipo de serviço de rede sem a

necessidade de configurações complexas, quer sejam HTTP, FTP, SSH, SMB e etc, em qualquer instancia do I2P, sem qualquer conhecimento avançado. Estes serviços são executados de forma anônima no interior da rede I2P e não são acessíveis aos usuários da internet, só para aqueles que estão na rede I2P.

O tráfico da I2P é cruzado por vários pontos de redes utilizando servidores proxy, onde toda sua rede é totalmente descentralizada e a informação encontra-se distribuída em múltiplos pontos da rede. É

uma rede orientada a mensagem onde cada pacote de dados é encriptado e enviado ao destinatário de forma anônima, ou seja, quando o emissor envia uma mensagem, os demais participantes que estão na rede não conhecem a existência dos usuários, conteúdos e destinatários da mensagem enviada.

A rede I2P é praticamente descentralizada, com exceção dos chamados "Reseed Servers", que são nada mais do que os servidores que servem como ponto de entrada da rede para novas conexões.

Assim que estiver conectado à rede, você só descobrirá pares construindo túneis "exploratórios", mas para fazer sua conexão inicial, você precisa obter um conjunto de pares de algum lugar.

Arquitetura

Quando um usuário se conecta na rede I2P, automaticamente se converte em um roteador, ou seja, cada usuário contribui com um pouco de sua largura de banda para outros usuários usarem a rede I2P.

Consequentemente se em determinado momento, na rede I2P

estiverem poucos usuários conectados, a rede ficará lenta pois não terá largura de banda.

O tuneis só funcionam em um único sentido, seja para enviar ou receber um pacote de dados, desde o emissor até o receptor e vice-versa. Por isso, para que uma instância de I2P possa enviar e/ou receber informações, deve-se criar tuneis de entrada e de saída, pois eles serão os responsáveis para enviar e receber pacotes de dados na I2P.

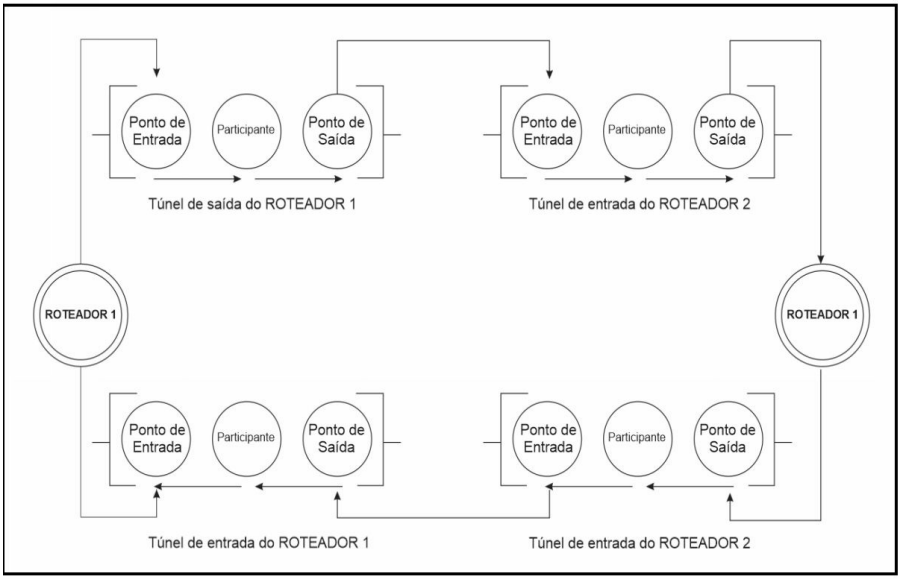


Figura 17: Arquitetura da rede I2P

No exemplo acima vemos que o ROTEADOR 1 está como emissor de mensagem que enviará ao primeiro roteador do túnel de saída (GATEWAY). O roteador posteriormente obtém a informação do outro nó do túnel, pois este roteador é um participante e ao mesmo tempo um "Gateway", e se encarregará de obter a direção do nó no túnel para enviar a mensagem.

O "Endpoint" se encarregará de obter a direção do "Gateway"

correspondente ao túnel de entrada do ROTEADOR 2. O túnel de entrada recebe a mensagem por parte do "Endpoint" e se encarrega de levar ao destino correspondente, por meio do túnel de entrada.

A rede I2P possui um banco de dados distribuído chamado de netDb, o qual contém apenas dois tipos de dados - informações de contato do roteador (RouterInfos) e informações de contato do

destino (LeaseSets).

Cada parte dos dados é assinada pela parte apropriada e verificada por qualquer pessoa que os use ou armazene. Além disso, os dados contêm informações vitalícias, permitindo que entradas irrelevantes sejam descartadas, entradas mais recentes substituam as mais antigas, sendo assim uma proteção contra rastreamento.

O netDb é distribuído com uma técnica simples chamada "floodfill", onde um subconjunto de todos os roteadores, denominado

"roteadores floodfill", mantém o banco de dados distribuído.

Instalando o I2P em um GNU/Linux

Apesar de estar disponível para Windows, Mac OS e Linux, iremos cobrir a instalação em ambientes GNU/Linux (Debian-like, como o Kali Linux). Para mais informações sobre a instalação em outros Sistemas Operacionais, acesse: geti2p.net/pt-br/download

Usando o seu terminal, execute os comandos abaixo para instalar o I2P:

apt-get update && apt-get install apt-transport-https curl

apt-get install i2p

Após a instalação, basta startar o serviço:

i2prouter start

A partir de agora o serviço I2P estará disponível na porta 7657, conforme imagem abaixo:

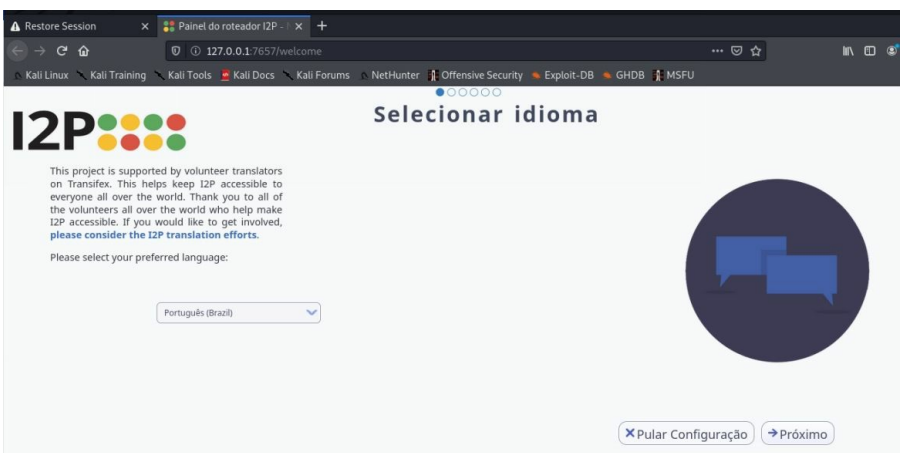


Figura 18: Funcionamento do I2P

Acessando a Dark Net através do Tor Browser

Nos capítulos anteriores, ensinamos a instalar o Tor e o browser TOR,

agora iremos configurá-lo utilizando algumas medidas de contrainteligência, dificultando ainda mais a rastreabilidade na rede TOR.

Um fato curioso sobre a rastreabilidade no Tor é que os desenvolvedores do TOR alegam que o navegador não rastreia o seu computador, no entanto se o seu computador não estiver na hora correta, o TOR não irá conectar aos relays da rede. Interessante isso não?!

Enfim, vamos as configurações. Como o Tor Browser é baseado no Firefox, você verá que muitas configurações se assemelham as que recomendamos serem realizadas no Firefox, anteriormente: Em **Preferências**, na aba **Pesquisa**, serão exibidos os mecanismos de pesquisa que aparecerão na barra de endereço. Deixe ativado somente o **DuckDuckGo**, **DuckDuckGoOnion** e o **Startpage.**

Acesse a página de configurações avançadas do **Tor Browser** digitando **about:config** na barra de endereços do seu navegador.

Uma mensagem de aviso aparecerá; aperte o botão "**Eu aceito o risco!**" para acessar o painel de configurações avançadas. Use o campo Pesquisar para procurar pelas configurações que iremos citar e poder alterá-las.

1. Cache do TOR Browser

Para começar, vamos alterar a primeira configuração chamada **browser.cache.disk_cache_ssl** para **false** (clique duas vezes para alterar o valor das configurações). Isso DESABILITA o cache em memória no browser.

Altere também a opção **browser.cache.memory.enable** para **false.**

2. Clipboad events

Essa chave permite que sites possam obter notificações caso o usuário copie, cole, ou recorte alguma coisa a partir de uma página Web.

Troque o **dom.event.clipboardevents.enabled** para **false.**

3. Kit de ferramentas de telemetria do navegador TOR.

Alterando para **false** as opções abaixo você diz ao navegador não enviar algumas informações de perfil, bem como enviar ping ao sair do browser ou acessar com um novo perfil.

• toolkit.telemetry.shutdownPingSender.enabled

• toolkit.telemetry.archive.enabled

• toolkit.telemetry.newProfilePing.enabled

4. Desabilitar o WEBRTC

Altere para **false** as opções abaixo para desabilitar o suporte ao Web-RTC em seu navegador:

• media.peerconnection.identity.enabled

• media.peerconnection.dtmf.enabled

• media.peerconnection.rtpsourcesapi.enabled

5. Instalar/ativar algumas extensões para aumentar a sua segurança.

As versões mais novas do Tor Browser já vem com algumas extensões de privacidade ativadas, tais como HTTPS Everywhere, NoScript, Privacy Badger e uBlock Origin. No entanto, não custa verificar se no seu caso elas estão instaladas e/ou ativas.

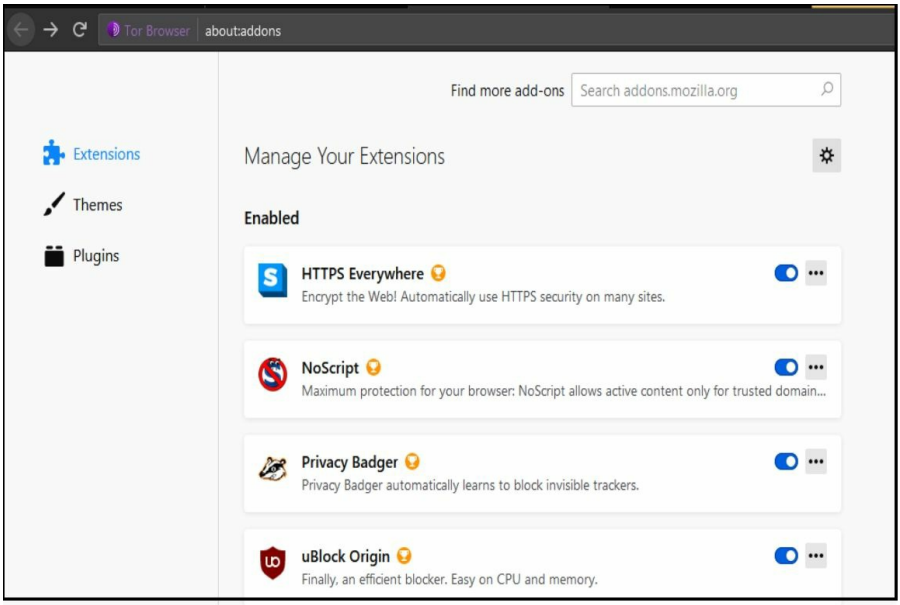


Figura 19: Extensões de privacidade para o Tor Broswser Realizadas todas estas configurações, agora iremos navegar na Darknet com segurança.

Abaixo cito uma lista de sites interessantes na Dark Net, tanto para ações de OPSEC quanto para conhecimento. No entanto, cabe ressaltar que alguns dos sites disponibilizados neste material poderão não estar online a depender do horário. Manter os sites offline por certos períodos é uma prática comum entre os donos de sites da Dark Net para evitar rastreamento.

1. Mecanismos de pesquisa:

• Ahmia (http://msydqstlz2kzerdg.onion/)

• Candle (http://gjobqjj7wyczbqie.onion/)

• Torch (http://xmh57jrzrnw6insl.onion/)

• Grams (http://grams7enufi7jmdl.onion/)

2. Sites para Bitcoin:

• EasyCoin (http://easycoinsayj7p5l.onion/)

• WeBuyBitcoins (http://jzn5w5pac26sqef4.onion/)

• OnionWallet (http://ow24et3tetp6tvmk.onion/)

3. Rede Social

• Atlayo (http://atlayofke5rqhsma.onion/)

• BlackBook (http://blkbook3fxhcsn3u.onion/)

• Daniel's Chat (http://danschatjr7qbwip.onion)

4. Serviço de Armazenamento

• Site: http://torsafeiwttlku16.onio/

Descrição: permite armazenamento de pasta de todos os tipos de forma segura e confidencial.

• Site: http://imgbifwwqoixh7te.onion/

Descrição:

serviço

de

upload

de

imagens

e

outros

compartilhamentos TOR.

• Site: http://wuvdsbmbwyjzsgei.onio/

Descrição: serviço para fazer download ou upload de qualquer música

5. Fórum, wikis e documentação

• Site: http://libraryqtlpitkix.onion/library/

Descrição: a livraria mais antiga da darknet;

• Site: http://xffmro77i3lixucja.onion/

Descrição: uma das livrarias online mais completa da rede TOR.

Boa opção para estudantes;

• Site: http://jwgkxry7xjeaeg5d.onion/

Descrição: leaks de informações sigilosas e de governos

• Site: http://hackerw6dcplg3ej.onion/

Descrição: site contendo vários livros e recursos sobre desenvolvimento de software, pentesting e hacking.

Acessando a Dark Net através da I2P

Antes de falarmos sobre a forma de acesso, um ponto importante que precisamos frisar é que na I2P não existe um sistema de resolução de nomes de domínios como o clássico DNS. Em segundo lugar, existe um sistema de nome básico que vem instalado em cada instancia de I2P que depende completamente de um arquivo de texto que aponta um domínio “I2P” para um hash base32 ou base64, e este hash é o que se conhece como o destino do serviço solicitado em questão.

Este serviço é chamado “SusiDNS”, e encontra-se em

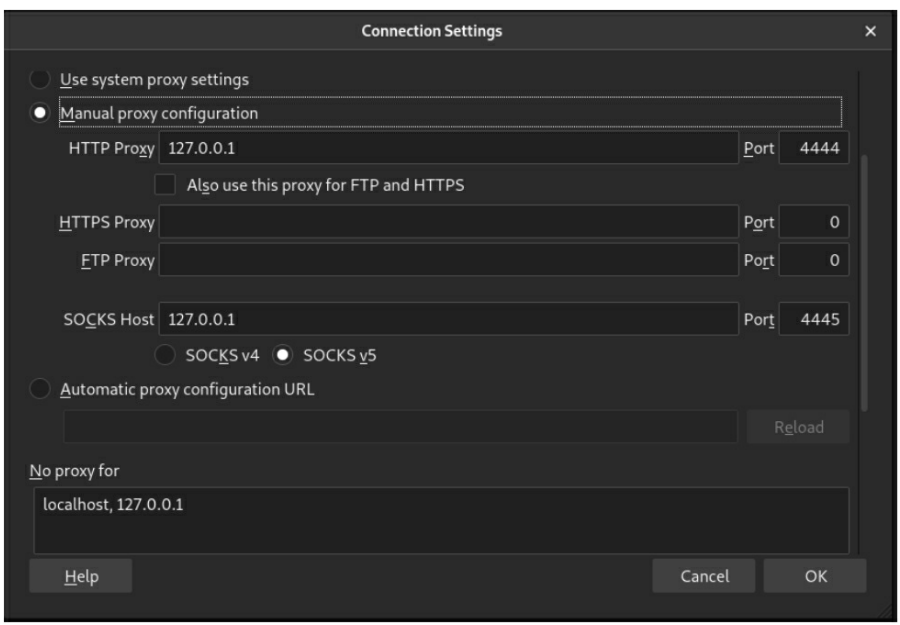
http://127.0.0.1:7657/susidns/index.

Já falamos que a rede I2P fornece suporte para qualquer tipo de serviço e protocolo de rede, no entanto os mais conhecidos são os serviços web - os quais na terminologia da I2P são conhecidos como

“EEPSites”. Um EEPSite é exatamente igual a qualquer serviço dos que se encontram disponíveis na internet, com uma única diferença: estão na rede I2P. Ele seria o análogo ao sites .onion que rodam na rede Tor.

A I2P é um pouco diferente do Tor, embora ambos tenham o mesmo objetivo. É tecnicamente possível configurar um nó de saída na I2P (chamado de outproxy na linguagem I2P), mas na prática a I2P geralmente não é usada dessa forma. Ela é quase exclusivamente usada para acessar sites EEPSites em vez de usá-lo como uma forma anônima de acessar a Internet pública – e do ponto de vista da rede em si, que gera um nível muito maior de anonimato do que a rede Tor, por exemplo.

Tudo que você precisa na I2P está no seu “roteador” – a página web acessível em http://127.0.0.1/7657. Enquanto o serviço roda em segundo plano, essa página faz a interface com esse serviço.



E o pontapé inicial para se acessar os EEPSites é configurar o proxy no seu navegador, o qual fará um roteamento interno no serviço da I2P rodando localmente. Para tal, usaremos a porta 4444 para as requisições HTTP e a porta 4445 para o protocolo SOCKS, conforme a imagem abaixo.

Figura 20: Configurando o proxy para utilizar a I2P para acesso a Dark Net Por fim, acesse a página de configurações avançadas do seu Firefox em **about:config**, aceite os termos e localize a chave **media.peerConnection.ice.proxy_only**.

Certifique-se de que esteja configurada como **true,** pois deverá estar com **false** como default.

Lembre-se de que a I2P é uma rede pequena e irregular, e os EEPSites geralmente são hospedados em computadores de usuários, logo podem ficar offline em determinados momentos.

Realizada todas essas configurações, agora iremos navegar na Dark Net utilizando a I2P. Abaixo cito alguns sites da Dark Net acessíveis através da I2P muito úteis para ações de OPSEC, bem como para agregar conhecimento.

Endereço I2P: tracker2.postman.i2p

Endereço

base32:

6a4kxkg5wp33p25qqhgwl6sj4yh4xuf5b3p3qldwgclebchm3eea
Descrição: um dos serviços mais conhecido de armazenamento via torrent em I2P.

Endereço I2P: identiguy.i2p

Endereço

base32:

3mzmrus2oron5fxptw7hw2puho3bnqmw2hqy7nw64dsrrjwdilva
Descrição: Wiki de EEPsites que mostra o status atualizado de sites na rede oculta de I2P.

Endereço I2P: planet.i2p

Endereço

base32:

pztcztaklof7s4me2vgtdddzesnunvk55zke6oz5e77ci3qk64yq
Descrição: Se trata de um site que inclui todas as novidades em I2P. Neste EEPsite podemos ver as versões de I2P disponíveis, as diferentes plataformas e arquiteturas que são desenvolvidas e alguns bugs nesta rede.

Endereço I2P: hq.postman.i2p

Endereço

base32:

7ewjvbcwgah57n64cwbsxqai7eutqofkesuxfsuhfheijivdjqra **Descrição:** serviço de I2P para criar conta de e-mail de forma anônima. Para utilizar esta conta, o cliente deverá estar conectado à rede I2P para envio e recebimento de e-mail.

Endereço I2P: pull.git.repo.i2p

Endereço

base32:

3so7htzxzz6h46qvjm3fbd735zl3lrblerlj2xxybhobublcv67q **Descrição:** É um site público de hospedagem com suporte ao Git.

Acessando a Dark Net através da

Freenet

O funcionamento da Freenet segue o mesmo esquema que a I2P, já que ambas têm soluções de anonimato que focam na criação de uma rede privada.

Do mesmo modo que a I2P, a Freenet é uma solução “inproxy”

que se encontra desenhada especificamente para criar e consumir serviços no interior de sua rede, mas não permite o acesso direto a internet por meio de “repetidores” como é o caso das outras soluções

“outproxy”, tais como o Tor.

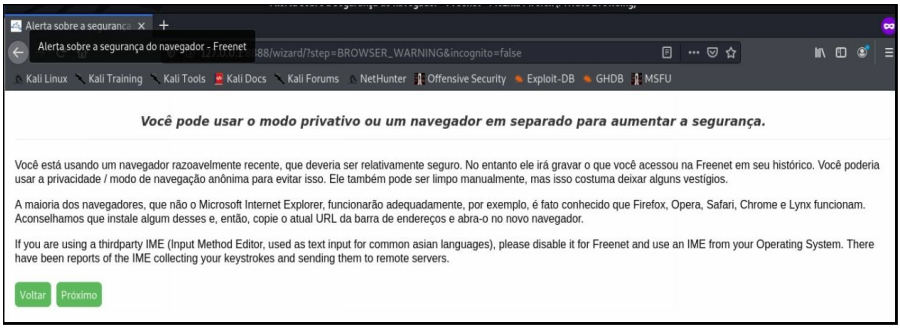
No capítulo sobre a instalação da Freenet vimos como configurar nosso ambiente para acessá-la, no entanto existe uma outra forma a qual citaremos neste passo-a-passo:

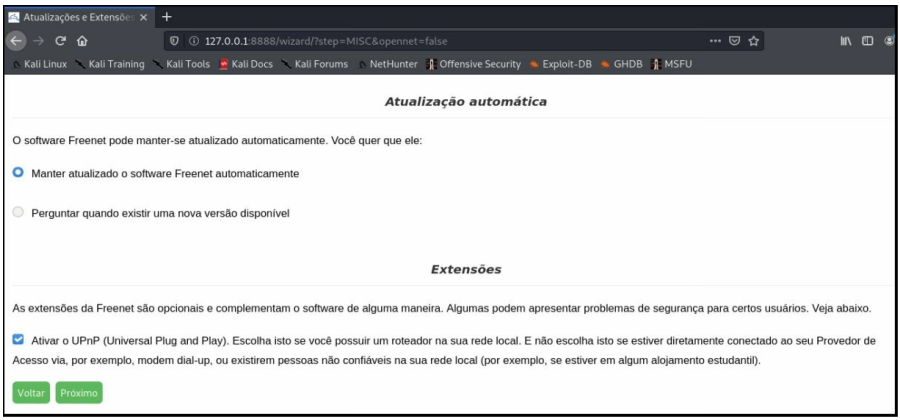
Localize o diretório **Freenet/bin** em seu sistema e execute o script **browser.sh**, o qual irá carregar o seu navegador padrão já na tela

inicial de configuração da Freenet.

Figura 21: Tela inicial da Freenet

Você sempre deve navegar na Freenet nos modos de navegação privada ou anônima. Se ainda não o fez, faça-o agora. Lembre-se de copiar o URL e colá-lo de volta na barra de endereço. Neste caso





vamos fazer uma configuração mais detalhada para termos acesso aos sites do Freenet.

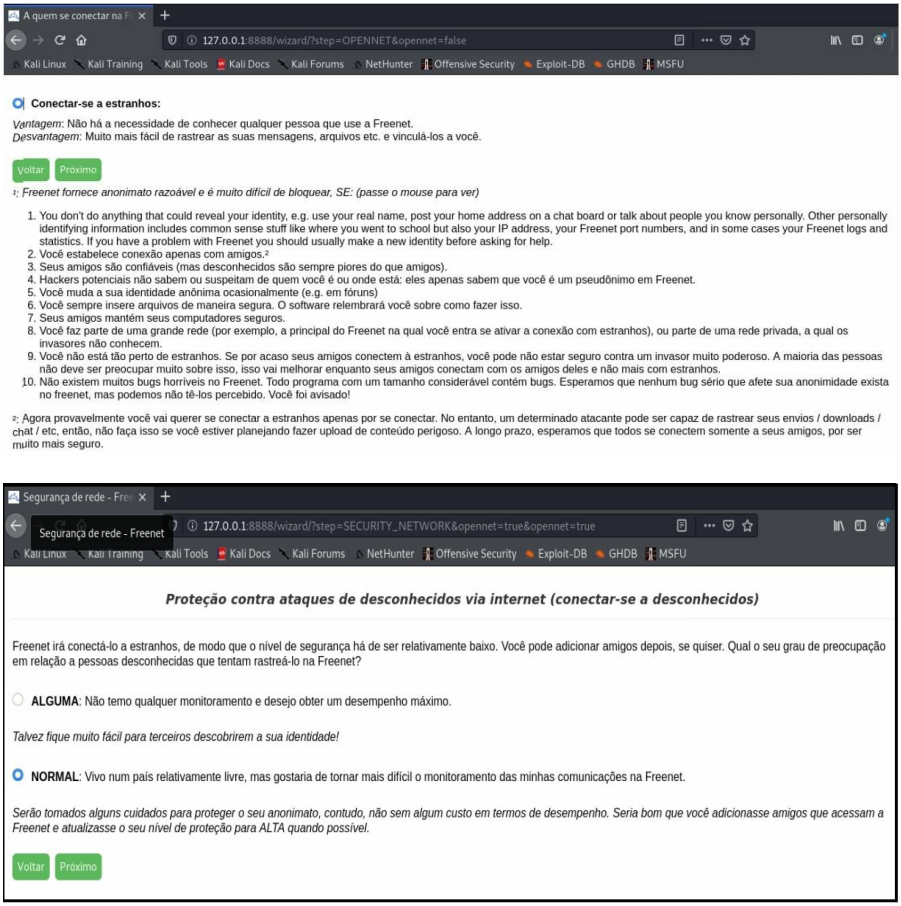
Figura 22: Modo anônimo na Freenet

Clique em 'Avançar' a menos que você tenha um motivo para desativar o UPnP.

Figura 23: Configuração de UPnP

Escolha a segunda opção aqui. Se você conhece outras pessoas que

usam Freenet, você pode atualizar para o modo Dark Net no

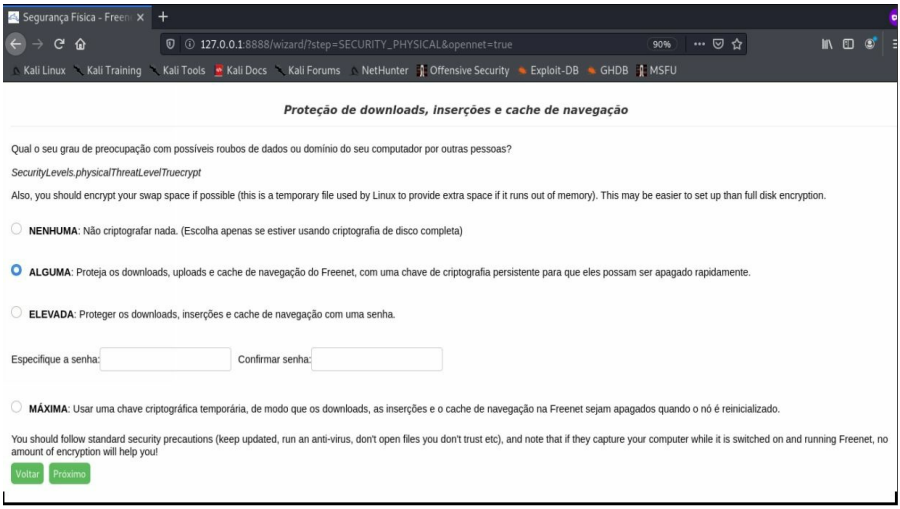


futuro, mas por enquanto você precisa se conectar a estranhos para acessar a rede.

Figura 24: Modo de conexão na Freenett

Na próxima tela (conforme abaixo) escolha a opção NORMAL.

Figura 25: Proteção contra ataques de desconhecidos na Freenet



Na próxima tela escolha a opção "BAIXO", a menos que já esteja usando criptografia de disco inteiro; nesse caso, você pode escolher "NENHUMA". Os níveis mais altos de segurança infelizmente não protegem totalmente sua identidade se você usar os tipos de plug-ins de rede social que iremos instalar.

Figura 26: Proteção contra ataques de desconhecidos na Freenet O instalador recomendará um valor padrão com base no tamanho do seu disco rígido. Você pode usar o valor que ele sugere ou selecionar algo diferente.

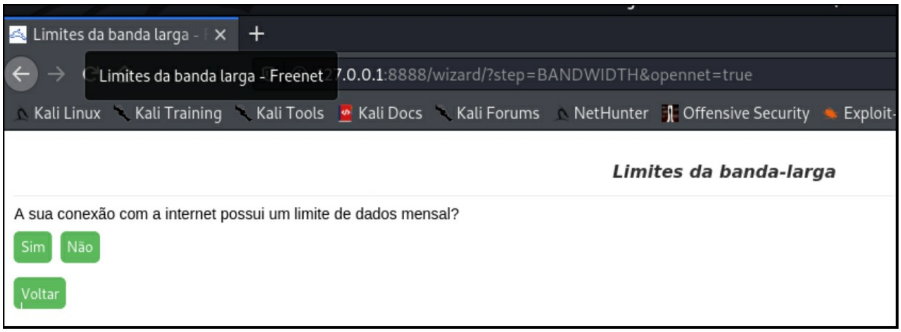


Figura 27: Quantidade de dados armazenados pela Freenet Você tem duas opções para escolher na próxima tela. Se você deseja limitar a largura de banda com base em um limite mensal, clique em 'Sim'. Caso contrário, clique em 'Não' e pule para a outra etapa.

Figura 28: Largura de banda na Freenet

Selecione' seu limite de dados mensal entre as opções fornecidas ou digite um valor na última caixa.

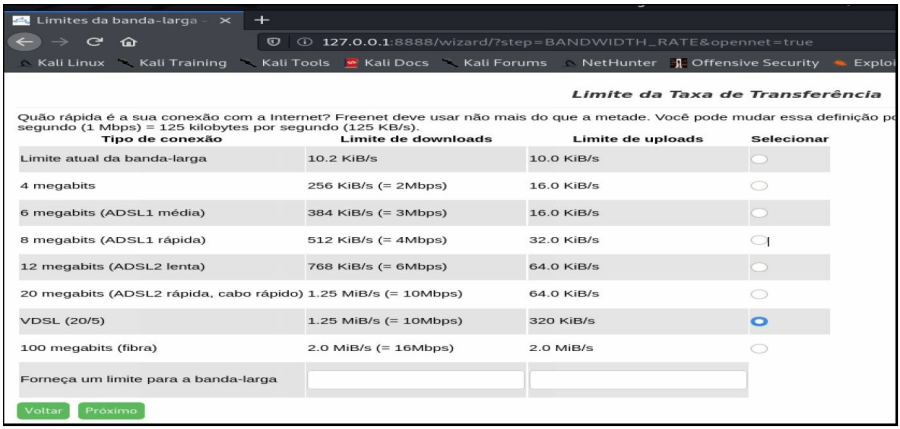


Figura 29: Limite mensal de dados

Selecione o limite de largura de banda correto com base no tipo de conexão em seus próprios valores.

Figura 29: Opções de largura de banda na Freenet

Seu nó agora está em execução. Antes de instalar qualquer um dos plug-ins de rede social em etapas futuras, você deve verificar a quantidade máxima de memória que seu nó pode usar.

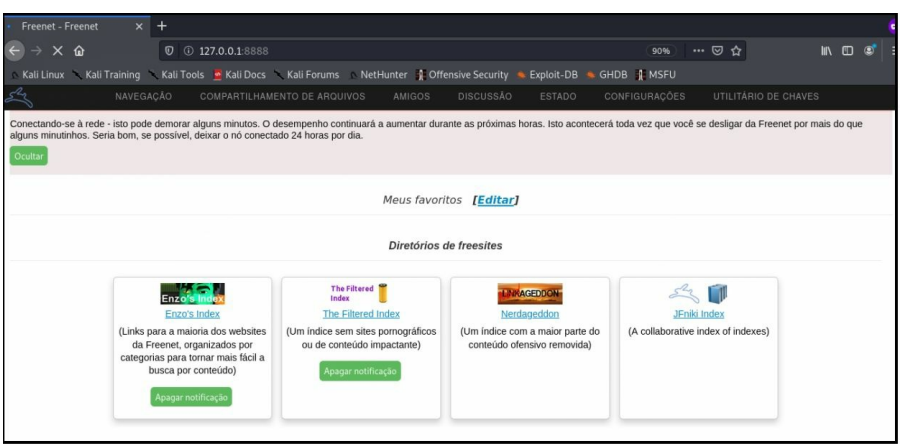


Figura 30: Plugins para a Freenet

Vá para a página "Especificação do Núcleo" do menu **Configuração**.

O instalador da Freenet escolheu um valor default para o "Uso máximo

da memória" e geralmente, esse valor é muito pequeno para executar os plugins que instalaremos nas etapas posteriores. Por tanto certifique-se de que este valor seja de pelo menos **512 MB**

para garantir que seu nó não fique sem memória.

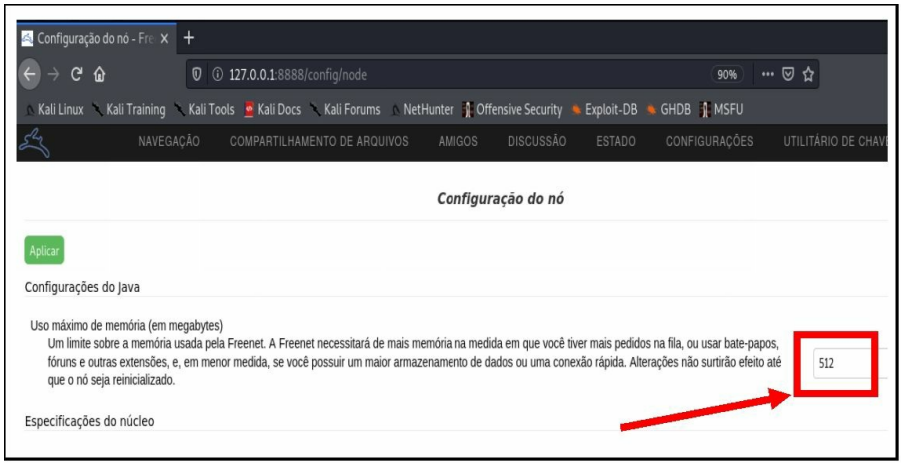


Figura 30: Configurações de memória pra Freenet

Se você não encontrar a seção **WRAPPER** e tiver seguido as instruções corretamente até aqui, fique tranquilo pois este é um bug da versão atual de quando foi escrito este material.

Para contornar este problema, procure o arquivo "**wrapper.conf**"

em seu computador e abra-o em um editor de texto. Encontre a linha começando com "**wrapper.java.maxmemory**" e certifique-se de que o valor seja de pelo menos **512**. Salve o arquivo e reinicie seu nó. Quando terminar, vá até o final da página e clique em 'Aplicar'.

Retorne à página inicial do nó para acessar o comando de reinicialização.

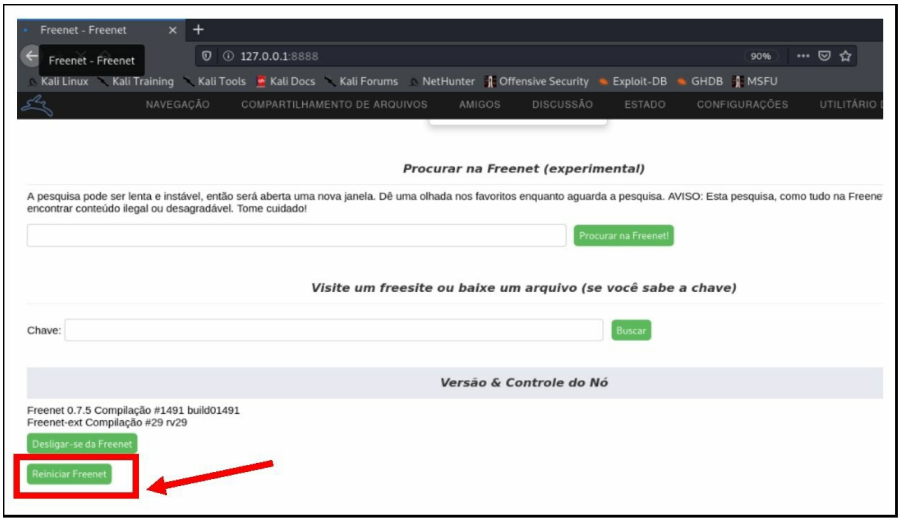


Figura 30: Configurações de memória pra Freenet

Reinicie o nó para atualizar a configuração de memória máxima.

Depois de todas essas configurações iniciais, temos que ter em mente que existem diferenças entre a rede TOR, a I2P e a Freenet, principalmente pois seus conteúdos só estão disponíveis na maior parte do tempo graças a sua arquitetura de rede anônima, e não obstante a isto, a disponibilidade destes conteúdos depende diretamente da quantidade de acessos que recebem e dos números de "datastore" em que se encontra hospedado.

Abaixo cito alguns repositórios interessantes na Freenet: **Nome do serviço:** BIBLIOTECA

Chave freenet:

http://localhost:8888/USK@ueGkuYERvLyWLwbDf-

fYNn~qIZR7KG~FNALH3DWpUyo,MEsM7dD-

r5ij6ePo9cXPS9CE4lhuEMRkZcykH-akvos,AQACAAE/calibre/10/

Nome do serviço: CHAN

Chave freenet:

http://localhost:8888/
freenet:USK@kSloth~SrrdJfe8qoumuiY7tWSVOpQav7usAwMB7PqE,JJRmnr
fmsarchive/25/

Nome do serviço: LINK AGEDDON

Chave freenet:

http://localhost:8888/freenet:USK@Isel-izgllc8sr~1reXQJz1LNGLIY

voOnLWWOyagYQ,xWfr4py0YZqAQSI-BX7bolDe-kI3DW~i9xHCHd-Bu9k,AQACAAE/linkageddon/1071/

Nome do serviço: DOCWIK

Chave freenet:

http://127.0.0.1:8888/freenet:USK@z6lnOx7PPe16P3Sobu1KM9jiLiIxdvE3L918QMVCLak,AmZ7Re

W4Zs38Ks511lRTsWleMj2mVAReB4E,AQACAAE/freenetdocwiki/17/

Nome do serviço: FREEMAIL

Chave freenet:

http://127.0.0.1:8888/freenet:USK@M0d8y6YoLpXOeQGxu0-IDg8sE5Yt~Ky6t~GPyyZe~zo,KlqIjAj3~dA1Zf57VDljkmp3vHUozndpxnH-P2RRugI,AQACAAE/freemail/8/

Nome do serviço: WIKI ANOTHER INDEX

Chave freenet:

http://127.0.0.1:8888/freenet:USK@zQyF2O1o8B4y40w7Twz8y2I9haW3d2DTlxjTHPu7zc8,h2mhQ

QOroBf5hrlbw,AQACAAE/AnotherIndex/104/

Anonimização com SPLITTER

Um dos principais objetivos das técnicas de anonimização é dar ao operador de OPSEC a capacidade de acessar a surface de forma anônima, ou seja, possibilitar a navegação na internet protegida por camadas de anonimização e, obviamente, tornar o processo de desanonimização o mais difícil possível. E como vimos até aqui, este processo não é fácil e quanto mais camadas de anonimização colocamos, mais dificultosa é a nossa navegabilidade na rede.

Partindo deste desafio um pesquisador brasileiro – com muita honra, prefaciador deste livro – Rener Alberto, desenvolveu uma tool open

source baseada na Rede TOR, a qual configura e aplica uma cadeia sistemática de soluções para dificultar as técnicas de desanonimização relacionadas ao TOR, garantindo uma melhor navegabilidade ao usuário.

Por padrão o SPLITTER funciona com soluções open source, tais como o Privoxy, HAProxy, bem como o próprio TOR, porem ele é escalável, podendo ser integrado a uma infraestrutura de rede distribuída de VPS e/ou VPNs de baixo custo, o que dificultaria ainda mais a análise de tráfegos mais específicos e não permitiria uma associação direta entre a rede TOR e o usuário.

Cada solução relacionada ao SPLITTER é aplicada em uma sequência sistemática, direcionando os pacotes TCP do navegador (ou outras aplicações), primeiro para o HAProxy, depois para o Privoxy e por fim para o TOR, onde após ser roteado pelo circuito TOR ativo atual, o pacote chega ao destino final. E obviamente, a resposta para este pacote TCP seguirá o caminho inverso.

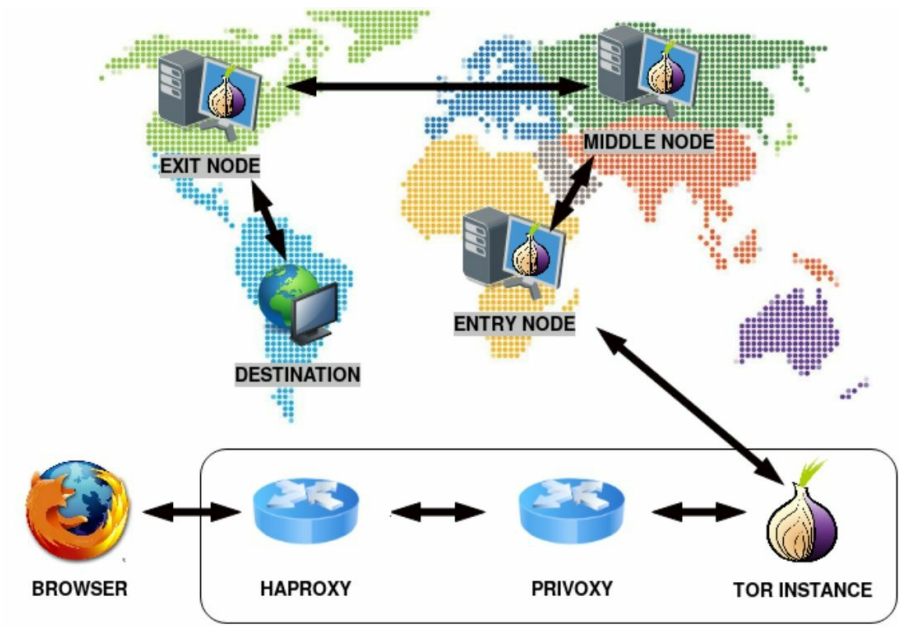


Figura 31: Topologia do funcionamento do SPLITTER

Não obstante aos benefícios do ponto de vista da conexão, o aspecto mais importante desta ferramenta é a abordagem de geolocalização e como ela seleciona os países que serão aplicados para compor o circuito TOR, pois ela permite ao usuário definir quantas instâncias do

TOR, quais e quantos países o SPLITTER

poderá usar. É possível, por exemplo, criar um número “X” de instâncias usando o mesmo país.

Instalação do SPLITTER no Kali Linux

O processo de instalação e uso do SPLITTER é simples, porém antes de iniciá-lo é necessário instalar as dependências conforme abaixo:

apt update & apt install tor privoxy haproxy proxychains expect

Efetue o download do SPLITTER e descompacte o tarball:

wget https://github.com/renergr1nch/splitter/blob/master/splitter_v.0.0.1.tar.gz

tar -xvf splitter_v.0.0.1.tar.gz && cd splitter_v0.0.1

A execução do SPLITTER deve ser feita desta forma:

./splitter.sh -i <INSTANCES> -c <COUNTRIES> -re entry Onde:

- **INSTANCE**: selecione a quantidade de circuitos TOR deseja utilizar

- **COUNTRIES**: selecione a quantidade de países deseja utilizar em cada instancia definida na opção anterior

Para

mais

informações

sobre

o

projeto,

visite:

https://github.com/renergr1nch/splitter

Open Source Intelligence (OSINT)

Dentre as diversas ações cibernéticas realizadas por um profissional de Cyber Security no campo da Inteligência e Contrainteligência, estão as

ações de coleta de dados no campo cibernético.

Relembremos o primeiro capítulo onde estudamos sobre as ações de inteligência na obtenção de dados. Ações estas que podem ser categorizadas como busca, quando necessitamos obter um dado protegido e que não está disponível de forma pública (atividade que geralmente envolve Engenharia Social, Invasão, desenvolvimento e implantação de malware e/ou backdoor e etc); e coleta, quando obtemos dados em fontes abertas, ou seja, através da exploração cibernética de fontes abertas (redes sociais, mecanismos de busca e etc) conseguimos obter os dados desejados. E é sobre as ações de coleta de dados que iremos discorrer neste capítulo.

Em atividades de OPSEC, a coleta e obtenção de dados e informações se dá de várias formas. As fontes de inteligência são classificadas de acordo com a natureza e a proveniência dos dados que elas fornecem, como já vimos anteriormente. Logo, a OSINT é um modelo de inteligência que visa coletar, processar e analisar informações provenientes de fontes públicas.

Esse tipo de inteligência tem se tornado mais importante e expressivo nas últimas décadas, com a expansão dos meios de comunicação, principalmente a rede mundial de computadores. Porém os Estados Unidos, por meio do departamento de OSINT da Central Intelligence Agency - CIA, já lida com esse tipo de dado desde a Segunda Guerra Mundial. E durante a Guerra Fria o Foreign Broadcast Information Service – FBIS (Serviço de Vigilância de Mídia Estrangeira) analisava e traduzia a maioria das publicações técnico científicas da União Soviética.

Uma das principais vantagens do uso do OSINT é o seu custo.

OSINT é muito mais barata do que as ferramentas tradicionais de coleta de inteligência e é particularmente adequada para organizações com orçamentos de inteligência limitados.

Em contrapartida, um dos maiores problemas do OSINT é seu potencial de sobrecarga de informações; A filtragem perceptiva do

"ruído" pode ser difícil. De fato sem ferramentas de OSINT valiosas, encontrar as informações corretas pode ser demorado. A OSINT

também não está pronta para uso e dificilmente pode ser automatizada como um todo. Ela requer muito trabalho de análise humana para distinguir informações válidas e verificadas, de notícias e informações falsas ou simplesmente incorretas.

Em relação a mentalidade de inteligência, quando um analista de inteligência iniciar sua pesquisa, precisará pensar em como localizar todos os dados necessários para chegar a uma determinada visão de inteligência. É fundamental que ele considere o uso de certas fontes e ferramentas, além de pesá-las umas contra as outras para tomar decisões. Deve-se manter os preconceitos pessoais fora do caso, pois eles fatalmente podem influenciar a pesquisa.

Levar em consideração os princípios da Inteligência é fundamental no trabalho de OSINT. Em todas as ações o analista tem que se fazer estas perguntas: Estou sendo objetivo? São estas as perguntas certas? Os dados fornecem tudo o que é necessário para responder à(s) pergunta(s)?

O pensamento crítico é fundamental para realizar uma pesquisa em OSINT. Tenha em mente que os dados coletados podem conter informações para enganá-lo. Por exemplo, notícias falsas, bots e etc.

Relatórios falsificados estão por toda parte. As fontes que você usa são confiáveis? E por que são consideradas confiáveis por você?

Sempre classifique suas fontes!

Metodologias para ações de OSINT

Descreveremos abaixo a metodologia aplicada em ações de OSINT, as quais são utilizadas pelas principais agências de inteligência do mundo.

Tenha sempre em mãos esse mindmap pois ele é extremamente útil em ações de OPSEC:

1. Escolha seu assunto de pesquisa (de preferência, faça uma entrada com seu cliente e defina a(s) pergunta(s). Defina uma pergunta “respondível”!

- Consiga-me tudo em Joãozinho não é respondível (o que é tudo?!)

- Joãozinho esteve na posição x com a pessoa y? É uma pergunta

“respondível”!

2. Faça o dever de casa sobre o assunto (conheça seu cliente e seu adversário)

3. Defina a questão principal de pesquisa, preferencialmente com um

subconjunto de perguntas. Utilize os 6 W's.

- o que (what)

- onde (where)

- quando (when)

- qual método (which method)

- quem (who)

- porque (why)

4. Definir fontes. (Google, Twitter, Facebook, Instagram, etc) 5. Reunir palavras-chave em cada questão de pesquisa.

6. Pense em quais ferramentas (OSINT) devem ser necessárias para esta pesquisa.

7. Pesquisa de verificação rápida (pesquisa de temporizador para evitar o afogamento em informações quando você realmente começa a pesquisar).

8. As descobertas preliminares são o que você esperava encontrar? Caso contrário, repita os passos 1 a 5.

9. Reúna as informações necessárias, exaura suas fontes.

10. Refine e analise as informações encontradas.

11. As descobertas secundárias são o que você esperava encontrar? Caso contrário, repita os passos 1 a 8.

12. Relatório. Inclua tudo! As coisas que você encontrou e analisou também as coisas que você não encontrou.

13. Deixe o relatório descansar, literalmente. Não envie imediatamente seu relatório.

14. Quando alguém voltar às suas conclusões/relatório com novas perguntas, repita todos os passos acima.

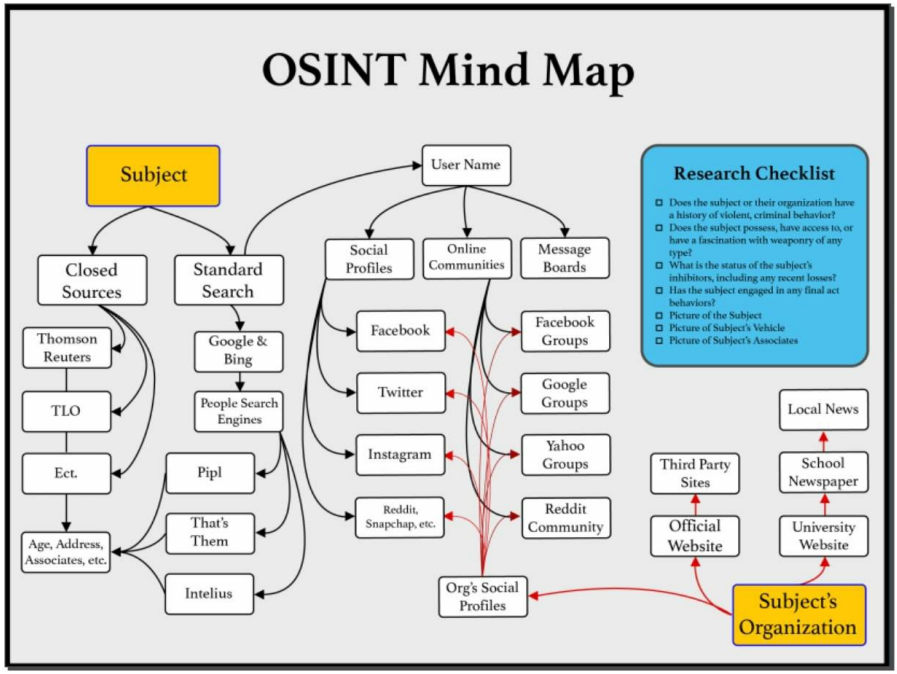


Figura 32: OSINT Mindmap

OSINT e Anonimização

O primeiro princípio da Inteligência é a segurança, e é com base neste princípio que as ações de OPSEC devem ser baseadas, tendo em vista que a segurança do analista (seus dados, sua identidade, localização e etc) deve ser resguardada a todo custo, inclusive em detrimento da ação de exploração.

Neste contexto faz-se necessário que sejam utilizadas as técnicas de anonimização em ações de OSINT uma vez que não somente o alvo pode vir a detectar o analista, mas também mecanismos de busca e sites que utilizem cookies. Pois como vimos anteriormente, através de correlação de tráfego, o fingerprint do analista pode ser detectado se a anonimização não for feita da forma correta.

Outro ponto importante nas ações de OSINT, levando-se em conta a anonimização, é a utilização de perfis fake. Redes sociais, como o Facebook por exemplo, utilizam o fingerprint do usuário para, dentre outros, fornecer conteúdo publicitário direcionado ao perfil deste, e do ponto de vista da segurança, isso é perigoso pois a identidade digital do usuário está sendo compartilhada entre a rede social e seus parceiros comerciais. Inclusive grandes vazamentos de dados

envolvendo o Facebook já foram descobertos, como o caso da Cambridge Analytics em 2018.

Dado a este fato, um analista de OSINT deve tomar o cuidado de utilizar perfis falsos para realização de suas ações exploratórias, além dos cuidados de anonimização de sua conexão. Estes perfis precisam ser criados com todo cuidado para que de forma alguma se chegue no analista em caso de auditorias de segurança e análises forenses.

Ferramentas de OSINT

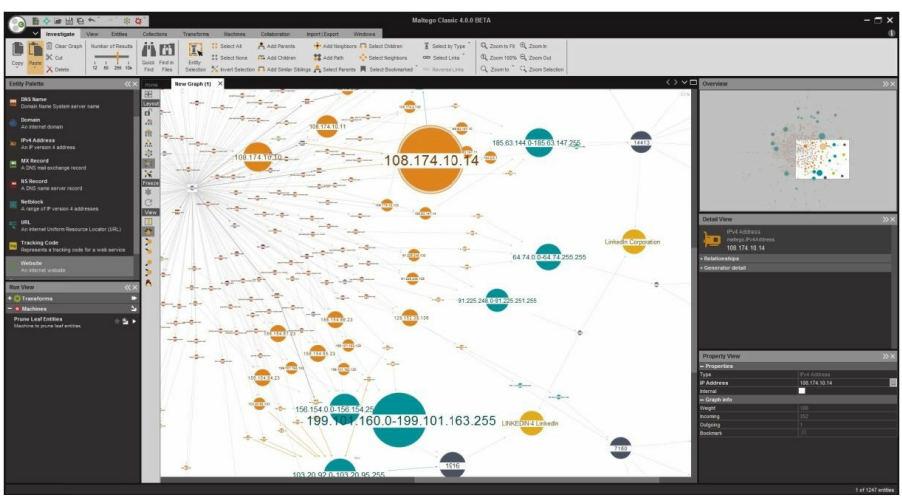
Para um analista de OPSEC, ter ferramentas confiáveis e que automatizem seu trabalho, é fundamental.

Devido a cultura do Software Livre, bem como a própria cultura Hacker, o compartilhamento de informações só aumenta na internet.

E por mais que citemos algumas ferramentas “consagradas”, é muito provável que você encontre um GitHub com algum “script” (ou até uma tool mais completa) que será mais útil pra você de que estas ferramentas citadas abaixo. Logo, antes de realizar alguma ação, não se limite ao que você conheçe de ferramentas. Use os conhecimentos de OSINT para aumentar o seu arsenal – com certeza tem muita coisa boa na internet surgindo diariamente.

a) Maltego

Maltego é um software que recolhe informações de várias fontes abertas (e pagas) e correlaciona os dados obtidos. Ele tem diversas vertentes, desde as análises de Redes Sociais, reconhecimentos de



DNS, passando por um excelente correlacionamento dos dados. O

Maltego é uma plataforma única que mostra de uma maneira muito simples, transparente e fácil todo o ambiente de uma organização/ rede.

Abaixo citamos alguns tipos de dados que podem ser coletados e correlacionados através do Maltego:

• Pessoas

• Grupos de pessoas/redes

• Companhias

• Organizações

• Websites

• Domínios

• DNS

• Blocos de AS

• Endereços de IP

• Palavras-chave

• Associações

• Arquivos

• E muito mais!

Figura 33: Maltego

b) TinEye

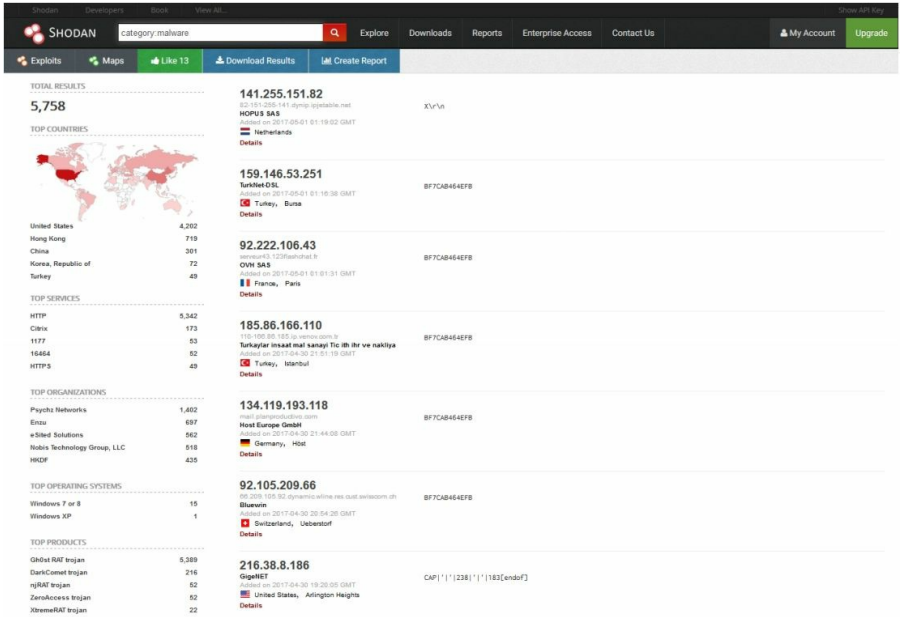
Ele é um serviço web de busca reversa por imagens, muito parecido com a busca por imagens do Google. Porém os seus diferenciais em relação ao serviço da gigante das buscas (além de pensar em sua privacidade) vão desde sua IA muito precisa até um banco muito maior de informações.

Ele está disponível em: https://tineye.com/

Figura 34: TinEye

c) Shodan

O Shodan é o primeiro serviço de busca que permite encontrar computadores e dispositivos conectados à rede. Inclua nessa lista webcams, roteadores domésticos e empresariais, smartphones,



tablets, telefones VoIP, computadores, servidores, sistemas de videoconferência e até outros como monitores de bebê e sistema de refrigeração de um prédio.

Além de informações sobre esses dispositivos, ele recolhe informações sobre diversos serviços, tais como HTTP, FTP, SSH, Telnet, SNMP, SIP, etc.

Um diferencial da plataforma é que, além de permitir pesquisas via web com a opção de Dorks, ele funciona muito bem via CLI, o que possibilita a automatização de tarefas, integração com outros serviços e etc.

Ele está disponível em: https://www.shodan.io/

Figura 35: Shodan

d) Google Hacking / Google Dorks O Google Hacking nada mais é que uma prática para encontrar arquivos, informações, dados e falhas em sites a partir do Google, usando -o como uma espécie de scanner, possibilitando manipular buscas avançadas por strings chamadas de “dorks” ou “operadores de pesquisa”.

Através das Dorks praticamente tudo que está disponível na internet pode ser buscado pelo Google, bastando saber passar os parâmetros corretos ao Google.

Seguem abaixo alguns exemplos de dorks:

- **intitle**: procura palavras-chave no título da página

- **inurl**: procura as palavras mencionadas no URL.

- **filetype**: é usado para encontrar tipos de arquivos.

- **ext**: pesquisa por extensões de arquivos específicas

- **intext**: ajuda a procurar texto específico na página.

As dorks podem ser usadas em conjunto para refinar uma pesquisa, como por exemplo:

- **inurl:.gov "login"** : irá exibir páginas que contenham o TLD

".gov" e o termo "login" em sua URL

- **site:.br +RG +CPF filetype:xls** : esta string irá pesquisar os sites com TLD ".br" que contenham arquivos XLS indexados, e este com dados que remetam a RG e CPF

- **site:.bv -.mil** : realiza pesquisas nos domínios do TLD ".br"

exceto (operador -) os domínios que contenham o TLD ".mil"

O universo das dorks vai muito além disso e ainda é atualizado constantemente pelo Google. Abaixo seguem algumas dicas de sites e repositórios que mantém atualizadas as informações sobre as dorks:

- Google Dorks List Collection for SQL Injection – SQL Dorks 2021:

https://gbhackers.com/latest-google-sql-dorks/

- Google Dorks List 2021 For Ethical Hacking and Penetration Testing: https://gbhackers.com/latest-google-dorks-list/

- Google Hacking Exploit Database: https://www.exploit-

db.com/google-hacking-database

e) GitHub Dorks

A pesquisa do GitHub é um recurso muito poderoso e útil que pode ser usado para buscar por dados confidenciais em um repositório. E através do uso de Dorks, podemos chegar em diversos dados

importantes, tais como credenciais, tokens de segurança, chaves privadas e muito mais.

Abaixo segue um exemplo das dorks básicas do GitHub:

- **filename**: busca por nomes de arquivos

- **extensions**: busca por extensões

- **path**: busca por caminhos

- **“palavra”** : busca exata pelo item entre aspas As dorks do GitHub também aceitam operadores lógicos, tais como **or**, **and** e **NOT**, Podendo serem utilizados assim:

- **extensions:php NOT "hello world"** : busca por arquivos de extensão **php** que não contenham a string **hello world**

- **extension:json mongolab.com** : busca por credenciais **mongolab** em arquivos **json**

- **filename:.env MAIL_HOST=smtp.gmail.com** : busca por arquivos que contenham **.env** em seu nome e possuam a string **MAIL_HOST=smtp.gmail.com**

Apesar de existirem ferramentas que automatizem o processo de buscas com Dorks no GitHubneste link existe uma lista não exaustiva de Dorks do GitHub: https://github.com/techgaun/github-dorks

f) Hunter.io

Ele é uma ferramenta de busca de endereços de e-mail, muito útil pra encontrar e-mails corporativo através de uma simples busca por um domínio. Ele utiliza um método de crawler em páginas web, combinado a bots que realizam pesquisas em diversos motores de busca a fim de encontrar ocorrências do domínio pesquisado.

https://hunter.io/

g) What is My Name

Ele é um serviço online de busca por usernames em diversos serviços na web, muito útil para correlacionar as ocorrências de um determinado nome de usuário em outros sites e serviços.

https://whatsmyname.app/

h) h8mail

Ele é uma tool de breach hunting, disponível no Git Hub, que realiza pesquisas em serviços e bases de leaks, tais como Have I Been Pwned, Hunter.io, Leak-Loop, IntelX.io, breachdirectorytk e etc.

https://github.com/khast3x/h8mail

i) Way Back Machine (Internet Archive)

Este é talvez um dos mais úteis serviços online no que diz respeito a coletar dados e informações que "já não estão disponíveis". Ele foi criado com o propósito de servir como um grande repositório de versões arquivadas de sites, no entanto é amplamente utilizado em ações de OSINT pois possibilita o acesso a versões antigas de um site,

as quais teriam sido excluídas.

Mas como estas informações seriam úteis sob a ótica da OSINT?

De diversas formas! Por exemplo: você pode coletar nomes, números de telefone, endereços de e-mail e até metadados de versões mais antigas de um site, os quais teriam sido excluídos por um determinado propósito. Em outros casos você pode até ter acesso a versões demo ou de desenvolvimento de um determinado site, a qual foi ao ar temporariamente para uma aprovação ou teste, por exemplo.

Estas versões muita das vezes possuem dados úteis, incluindo credenciais expostas.

https://archive.org/web/

j) Ahmia.fi

O Ahmia é um "Google da Dark Net" responsável por realizar buscas exclusivamente em hidden services na Rede Tor, ideal para pesquisas sobre leaks. Seu código é aberto e está disponível em

https://ahmia.fi/

Técnicas de Busca de Dados Negados Até aqui nos aprofundamos nos conceitos da Inteligência e Contrainteligência no âmbito da OPSEC, mergulhamos nas técnicas de coleta de dados de fontes humanas (PNL, Rapport, Persuasão e etc) e Cibernéticas (OSINT), bem como nas técnicas de Contrainteligência (Anonimização, uso da Deep Web e Dark Net e etc), ou seja, técnicas que visam proteger a nossa

privacidade e aumentar nossa segurança.

Mas e as técnicas de busca de dados negados em fontes cibernéticas – como ir além da OSINT e obter informações que não estão disponíveis abertamente?

Antes de respondermos a estes questionamentos, é importante frisarmos um ponto: as ações de Inteligência geralmente caminham na linha tênue entre o certo e o errado, entre o moral e o imoral, com o intuito de obterem ou protegerem seu bem de maior valor: a informação. Muitas agências de Inteligência utilizam-se de técnicas operacionais duvidosas do ponto de vista da moralidade (e até da Lei).

Um filme que é muito utilizado nas comunidades de Inteligência para exemplificar alguns tipos de técnicas operacionais é o **Operação Red Sparrow**, onde a personagem principal é uma agente Russa que se apaixona por um agente de CIA e se torna uma agente dupla.

Não obstante ao "hollywoodianismo" no pano de fundo do filme, ele retrata (dentre outras) uma técnica operacional muito utilizada pelas agências de Inteligência da Rússia – a manipulação do sexo oposto. Inclusive o filme é baseado no livro **Historical Dictionary of Sexspionage (Scarecrow Press)** de Nigel West, um historiador de espionagem, que trouxe a tona o tema, mesmo tendo sido praticamente "cancelado" pelo jornal **Daily Telegraph** em uma matéria que questiona a veracidade das informações levantadas por

Nigel em seu livro (por acaso lhe pareceu uma ação de Contrainteligência para desconstruir a informação descoberta pelo autor?).

O fato é: independente do seu estado de mente perante a verdade, técnicas de busca de dados negados estão sendo utilizadas agora mesmo em algum lugar do mundo enquanto você lê este livro.

Inclusive em empresas que vendem os serviços de inteligência e não possuem um governo por trás para resguardar suas ações.

Obviamente que minha intenção aqui não é lhe ensinar a cometer algum tipo de crime, pelo contrário. Nossa Lei é muito clara e severa em vários aspectos e sim, precisamos seguí-la. Logo o grande objetivo é lhe mostrar possibilidades… abrir sua mente, inclusive para que esteja atento, pois você pode ser um alvo de ações deste tipo.

Começando pelo início

O primeiro passo para realizar ações de busca de dados em fontes cibernéticas é prestar muita atenção quanto as técnicas de Contrainteligência que visam lhe proteger, acima de tudo. Inclusive este é um dos princípios da Inteligência que vimos no início do livro –

a Segurança. Um "agente" (operador de OPSEC) precisa colocar a sua segurança acima de tudo, inclusive da operação. Logo, antes de prosseguir no tema, volte nas técnicas de anonimização e faça o seu

"dever de casa" bem feito.

Se estamos falando de fontes cibernéticas, obviamente precisamos entender alguns princípios. E para isso vamos tentar responder os questionamentos abaixo:

- **Atualmente, qual é o local na Internet onde as pessoas mais se relacionam?** Nas Redes Sociais.

- **Toda Rede Social (ou as principais) são abertas e eu consigo ter acesso a todos os dados mesmo sem ao menos possuir uma conta?** Não. Muitas redes, principalmente as maiores como Facebook e Instagram, só conseguimos ver parte dos dados (as

vezes nem isso) sem estar logado na plataforma.

- **Já que precisarei logar nas Redes Sociais, posso usar minhas contas pessoais?** Obviamente que não!

- **E se vou ter que criar outra conta pra acessar uma Rede Social, quais os pré-requisitos básicos?** "Ser uma pessoa" e ter um endereço e e-mail e/ou telefone.

Podíamos seguir com mais proposições para embasarem nossas ações, mas até aqui conseguimos uma boa base para o nosso kick-off.

Já entendemos que precisaremos "estar" nas Redes Sociais, ter uma conta e os pré-requisitos para poder criar esta conta, correto?

Antes de discutirmos tecnicamente "o como" fazer isso, precisamos definir "o quem". A maioria das Redes Sociais possui mecanismos de verificação para identificar contas falsas (ou fake).

Não vamos citar aqui os motivos, pois alguns deles são bem óbvios, porém é fato que "precisamos ser uma pessoa" para ter uma conta.

Ou melhor dizendo: se quisermos buscar dados, ou seja, ir atrás do

que não está público (e isso envolve, muitas das vezes, se relacionar com pessoas na Internet fingindo ser outra pessoa), precisamos que nosso perfil engane os mecanismos de verificação de perfis fake. E

pra isso vamos ao nosso segundo ponto.

Estória de Cobertura

Esta é uma técnica operacional muito difundida entre as comunidades de Inteligência, pois praticamente todo agente de Inteligência tem a(s) sua(s) Estória de Cobertura.

Ela nada mais é do que uma Persona criada e alimentada para um fim, ou seja, um personagem que possui uma "vida própria" com informações corriqueiras que seriam fáceis de checar para não levantarem suspeitas.

Não vamos nos ater muito neste aspecto, até por que daria mais um livro. Mas o ponto aqui é: não adianta só criar um perfil fake, você

precisa dar a este perfil condições de, em uma checagem rápida, ele aparentar ser fidedigno. E obviamente que esta persona vai depender muito da ação, por exemplo: se o objetivo é buscar dados negados de um alvo que se interesse por mulheres, por exemplo, a forma mais factível deste alvo aceitar sua conexão em uma Rede Social seria uma persona feminina.

E aqui vai outra dica: a busca de dados negados é uma atividade que só deve ser realizada em último caso. Ou seja, se através da coleta de dados você não obteve muito sucesso, dai sim seria o caso de estudar a utilização da busca. Eu me refiro a "estudar a utilização"

pois, além de avaliar os impactos dessa ação, decidir fazer uma busca requer prioritariamente que se tenha um dossiê do alvo.

Um exemplo claro disso são em ações onde se é necessário realizar uma ação de Wi-Fi hacking contra determinado alvo e descobre-se que o protocolo de criptografa da rede é WPA2, por exemplo. Este é um protocolo que requer técnicas de ataque de desautenticação para captura de handshakes, os quais serão armazenados e testados através de outra técnica chamada de password guessing para tentar se obter a senha da rede. E se estou falando de password guessing, obviamente eu preciso de um dicionário de senhas. Há quem ache que um "rockyou.txt" (uma das mais famosas wordlists do mundo, amplamente utilizada em CTFs) vai ter a senha da rede do seu alvo. Lhe asseguro que, na maioria dos casos, não!

Seria preciso montar uma wordlist baseada nas informações do alvo (nome, cidade onde nasceu, nome dos filhos, esposas, pais, pets, placa do carro e etc). A possibilidade de sucesso através de uma wordlist criada através de um estudo prévio de OSINT é absurdamente maior.

Um off-topic rápido: uma tool incrível que auxilia no processo de criação deste tipo de wordlist é o **cupp** (nativo do Kali Linux). Com a flag **-i** (cupp -i) é possível utilizar um terminal interativo para fornecer

os dados do alvo, bem como acrescentar caracteres especiais, números no lugar de letras e etc.

Definido “o quem”, iremos passar para “o como”.

Criando perfis fake

Em nosso questionário respondido anteriormente nós entendemos alguns pré-requisitos técnicos para podermos criar um perfil em Rede Social. E a partir daqui daremos algumas dicas de serviços que poderão ser úteis neste processo.

No início talvez seja difícil criar esta Persona com todos os detalhes importantes que um indivíduo deve ter, bem como o que minimamente compartilhar em uma Rede Social. Se este é o seu caso, o site fakedetail.com/ pode lhe auxiliar neste processo. Ele é uma das principais plataformas de criação de Persona online, o qual te possibilita criar a sua praticamente do zero. Ele inclui ainda serviços de Deep Fake pra criação de posts, gerador de IMEIs aleatórios, gerador de conversas de chat, serviço de e-mail e etc.

a) Contas de e-mail

Antes de falarmos sobre como criar estas contas é importante citar um erro muito comum cometido por iniciantes no tema: reaproveitamento de contas de e-mail.

Cada perfil criado precisa obrigatoriamente ter apenas uma conta de e-mail atrelada. Não podemos reutilizar contas de e-mail para criação de outros perfis, mesmo que sejam em redes diferentes. Não só os serviços que rastreiam dados seriam o nosso perigo, mas em um caso de um comprometimento da conta de e-mail, seria fácil (através do correlacionamento) provar que o e-mail X pertence aos perfis Y e Z das Redes Sociais A e B.

Existem diversos sites que permitem a criação de contas de e-mail, inclusive temporárias, tais como:

- temp-mail.org/pt/

- mail.tm/pt/

- tempmailo.com/

E há quem prefira criar contas através de serviços que primam por privacidade, como é o caso do ProtonMail. O problema aqui é que algumas Redes Sociais proíbem a criação de contas a partir de endereços do ProtonMail ou serviços de e-mail temporários. E em outros casos, até lhe permitem criar a conta, no entanto lhe colocam em uma "quarentena velada" onde farão outros tipos de verificação posterior da sua conta – em outras palavras, você já estará gerando alertas desnecessários.

A dica é criar contas a partir de serviços de e-mail válidos, como Gmail e Hotmail, por exemplo. E claro, alguns deles pedem números de telefone para criar/validar a conta – e este será o nosso próximo tema.

b) número de celular

O principal método de verificação de conta através de números de celular é o SMS. E assim como o e-mail, também existem serviços online que permitem o recebimento de SMS grátis, tais como:

- freereceivesms.com/en/

- getfreesmsnumber.com/

- smscodeonline.com/

Claro que existem alguns pontos de observação nestes serviços:

- suas mensagens não são privadas. Eles disponibilizam páginas web onde todos conseguem ter acesso as mensagens recebidas.

- se é grátis, você é o produto. Ao acessar estes serviços garanta

que sua anonimização está num nível aceitável.

- boa parte destes números já estão em blacklist de grandes serviços na internet. Logo, a dica é achar um número relativamente novo.

Como comentei anteriormente, estamos na linha tênue entre o certo e o errado. Existem técnicas que envolvem atividades ilícitas para se obter números de celular "irrastreáveis", porém a minha dica é: assim

como comentamos nos capítulos sobre Anonimização e Fingerprint, as Redes Sociais identificam a origem do seu tráfego para, dentre outras coisas, verificar a coerência nos dados de cadastro. Ou seja, um tráfego identificado como sendo das Bahamas e um cadastro com um número com código internacional +55 (Brasil) é no mínimo suspeito.

c) Fotos

Se você chegou até aqui creio que já montou sua estória de cobertura para criação do seu perfil. E baseada nela, você irá precisar de imagens para seu perfil nas Rede Sociais.

Existem alguns serviços que geram imagens aleatórias baseadas em IA usando Deep Fake e podem ser úteis no início, como por exemplo:

- generated.photos/ : gerador de imagens de pessoas baseado em IA. Cria imagens de pessoas que não existem na realidade.

- generatestatus.com/generate-fake-instagram-post/ : cria posts fakes para o Instagram e Facebook. É bem interessante, pois você consegue upar uma imagem de perfil (pode ser a criada no serviço anterior) e uma imagem de fundo, e ele cria uma montagem usando as duas imagens.

Porém lembre-se que não basta criar o perfil, é preciso mantê-lo, e do ponto de vista de alimentá-lo com imagens, isso pode ser feito de

algumas formas, por exemplo:

- Lembra do TinEye que comentamos no capítulo de OSINT? Ao gerar uma imagem aleatória por IA, você pode buscar por imagens semelhantes a sua no TinEye e assim ter um “banco de fotos” para postar em seu novo perfil. Claro que as imagens não serão idênticas, mas para um processo de verificação básico, servem.

- Não use imagens que detalhem muito o rosto, desta forma será mais fácil achar outras semelhantes na internet.

- Procure imagens do dia-a-dia. Coisas que sua persona (uma pessoa comum) postaria na Internet. E se o seu perfil for no Instagram, ficou mais fácil. Muitas pessoas postam fotos de paisagens, restaurantes e etc. Lembre-se que as fotos não precisam ser da “mesma pessoa” da foto inicial, mas precisam dar a entender que sejam.

Uma IA sempre vai assemelhar-se ao modo de pensar de um ser humano, logo algumas técnicas de PNL também podem ser usadas

para manipular os sistemas de verificação. Se sua persona é um homem negro, por exemplo, achar uma foto na internet de pessoas em um restaurante, onde o fotógrafo está em primeira pessoa e só exibe a mão e o braço, pode ser uma foto interessante que induza a IA a entender que seu perfil não seja fake.

- Os sistemas de verificação são simples, não são investigações da CIA. Seja simplista, quanto menos informação detalhada e fácil de checar, melhor será o seu perfil.

Com o perfil criado e checado, agora vem a alimentação das informações. Obedeça sempre os traços da sua persona ao alimentar o perfil de informações. Exemplo: se sua persona é um homem com o corpo malhado, compartilhe (e interaja com postagens) que denotem gostos por esportes, academia e etc. Fale sobre isso, viva o seu personagem.

E como identificar um perfil fake?

Apesar de não ser o objetivo do capítulo, acho válido comentarmos sobre o tema, pois muitos usuários vem sendo vítimas de golpes na Internet através de perfis falsos.

O Facebook estima que existam aproximadamente 140 milhões de contas que “não são de pessoas reais”, e aqui podemos entender que não são somente contas fake, mas também contas de empresas e organizações que deveriam estar utilizando a plataforma através de páginas (Facebook Pages) ao invés de perfis.

Outro ponto que podemos confirmar (como comentamos antes) é que sim, existe uma verificação de perfis que, não só identifica os potenciais perfis falsos, mas também não os deleta.

Obviamente que, a depender do nível de expertise de quem criou o perfil falso, identificar pontos que ao mínimo nos coloquem uma

“pulga atrás da orelha” quanto a veracidade de um perfil, não é algo muito difícil de se fazer, como veremos abaixo:

- **Atente para a foto do perfil**. Contas falsas geralmente usam avatares ou imagens copiadas da internet como fotos de perfil. A dica é fazer uma busca na internet pela imagem do perfil para ver se ela está vinculada a alguma outra conta, por exemplo.

- **Quem são os seguidores?** Veja a quantidade e o tipo de seguidores que a conta suspeita possui. Se houverem muitas contas falsas

seguindo a conta suspeita, muito provavelmente a conta em questão também é falsa. Um outro comportamento comum em contas falsas é pagar pessoas reais para se envolverem com ela, logo se você identificar muitos emojis, comentários genéricos ou fora do tema, isso pode indicar que os comentários dos seguidores foram comprados e que a conta é falsa.

- **Confira o conteúdo**. Contas falsas geralmente espalham informações falsas e enchem seus feeds com memes e outras imagens reaproveitadas da Internet. Postagens sem conteúdo escrito ou visões unilaterais e extremas podem ser sinais de uma conta falsa.

Identificar contas falsas requer uma visão muito mais holística e de monitoração do que somente estes pontos comentados acima, principalmente se estivermos lidando com profissionais que usem os conhecimentos de Inteligência e OPSEC para criar e manter seus perfis. No entanto, na maioria dos casos os golpes são realizados por pessoas com baixa maturidade no tema, e seguir estes pontos acima podem lhe auxiliar muito no processo de detecção.

Outro ponto importante, do ponto de vista das ações de OPSEC, é que saber quais são os pontos de verificação de possíveis contas falsas pode lhe ajudar a melhorar o seu perfil.

Conclusão

Chegamos ao final desta jornada, caro leitor. E sinceramente espero que tenha sido uma jornada de aprendizagem, mas principalmente, de desenvolvimento de mindset.

Os conhecimentos de Inteligência e Contrainteligência são úteis para todos que entendam a importância da sua privacidade e que levem suas informações a sério – sejam elas pessoais ou corporativas.

Pessoalmente, o meu maior objetivo com a produção desta obra é que você saia desta imersão com a mente mais aberta e o mais fora da caixa possível. Que enxergue o mundo com outros olhos e nunca se esqueça: nem tudo que reluz é ouro. Tudo é uma questão de ponto de vista; do estado da sua mente perante a verdade.

Referências

NSA. **Purple Dragon: The Origin and Development of the United**

States

OPSEC

Program.

1993.

Disponível

em:

https://www.nsa.gov/portals/75/documents/news-

features/declassified-documents/cryptologic-

histories/purple_dragon.pdf. Acessado em: 03 Fev 2022.

ALLEN,

Steve.

Técnicas

proibidas

de

persuasão,

manipulação e influência usando os padrões de linguagem e técnicas de PNL. EUA: CreateSpace, 2018.

ECHEVERRI, Daniel. **Deep Web: TOR, FreeNET & I2P**.

Mósteles: Oxword, 2016. 238 p.

ROBERTSON, John et al. **Darkweb Cyber Threat Intelligence Mining**. London: Cambridge University Press, 2019. 150 p.

MARAS, Marie Helen; SECURITY, Department Of; JUSTICE, John Jay College Of Criminal. **The Darknet and Smarter Crime**.

Edinburg, Uk: Palgrave Macmillan, 2017. 246 p.

VAZ, Asael da Silva. **Proposta de Procedimentos para Anonimização da Origem de Ataques Cibernéticos.** 2018.

Disponível em: <http://bdex.eb.mil.br/jspui/handle/1/2642>. Acesso em: 18 Dez 2018.

MENDES, Diogo Carvalho. **Técnicas de Hacking para Anonimização na Internet.** 2014. Disponível em: <https://repositorio.ucp.pt/handle/10400.14/15325>. Acesso em: 18 Dez 2018.

FREITAS, Daniel Ferreira e COSTA, Vinícius Rodrigues. **O Uso de Fontes Abertas no Trabalho de Inteligência Policial.** 2018. Disponível em: <https://acervodigital.ssp.go.gov.br/pmgo/handle/123456789/1204>. Acesso em: 19 Dez 2018.

SETZER, Waldemar W. **Dado, Informação, Conhecimento e Competência**. 1999. Disponível em: https://www.academia.edu/download/44270487/ART_2_GEST.pdf. Acessado em: 03 Fev 2022.

Document Outline

- OPSEC
- Sobre o Autor
- Prefácio
- Introdução
- Princípios da Inteligência
- A Produção do Conhecimento
- Low Profile as a Lyfestyle
- Segurança como Valor Estratégico
- Engenharia Social
- Programação Neurolinguística
- Praticando o PNL: Rapport e Âncora
- Técnicas de Argumentação e Convencimento
- Fundamentos da Anonimização
- Fingerprint
- Conhecendo as camadas da Internet
- Rede Tor
- Rede Privada Virtual (VPN)
- Freenet
- Invisible Internet Project (I2P)
- Acessando a Dark Net através do Tor Browser
- Acessando a Dark Net através da I2P
- Acessando a Dark Net através da Freenet
- Anonimização com SPLITTER
- Open Source Intelligence (OSINT)
- Técnicas de Busca de Dados Negados
- Conclusão
- Referências